Universidade de Brasília
Instituto de Relações Internacionais (IREL)
Programa de Doutorado

Governança multisetorial e o processo de governança da internet: um estudo de caso sobre crime cibernético e filtragem na internet entre 1990 e 2010.

Daniel Oppermann

2012

Governança multisetorial e o processo de governança da internet: um estudo de caso sobre crime cibernético e filtragem na internet entre 1990 e 2010.

Daniel Oppermann

Tese apresentada ao Instituto de Relações Internacionais da Universidade de Brasília como requisito parcial à obtenção do título de Doutor em Relações Internacionais.

Orientador: Professor Dr. Estevão Chaves de Rezende Martins

RESUMO

Com o desenvolvimento do código HTML e do primeiro browser no começo dos anos 90, a internet deixou de ser uma rede acessada somente por um grupo relativamente pequeno de pessoas distribuídas por alguns países. A partir do momento em que houve a comercialização da internet, um número crescente de pessoas e atores começou a utilizar esse meio de forma a desenvolver suas próprias visões, ideias e interesses. O que começou como uma rede fundamentalmente usada por programadores e acadêmicos com o objetivo de criar acesso rápido a informações independentes da localização física do usuário se tranformou em uma rede de negócios, um meio de divulgação de direitos básicos, um fórum para qualquer tipo de informação, mas também um espaço para atividades mal intencionadas, crime cibernético ou ataques virtuais. Face a essa alta quantidade de problemas e oportunidades, um grande número de atores do setor público, do setor privado e da sociedade civil criou um novo fenômeno chamado governança de internet, baseado no conceito multi-setorial. A institucionalização desse processo aconteceu quando, em 2005, foi criado o Fórum de Governança de Internet pela Organização das Nações Unidas. Esta tese busca analisar o processo que criou o ambiente multi-setorial da governança de internet com foco nos dois fenômenos de crime cibernético e filtragem da internet.

ABSTRACT

With the development of HTML and the first browser in the beginning of the 1990s, the Internet was no longer a network exclusively for a relatively small group of individuals in a number of countries. With the commercialization of the Internet a growing number of individuals and actors started using this means to develop and follow their own visions, ideas and interests. What had started as a network basically used by programmers and scientists aiming at creating fast access to information independently of the physical location of the user, turned into a business network, a place to divulge basic rights, a forum for any kind of information but also a place for malicious activities, cybercrime, and virtual attacks. Given the high quantity of problems and opportunities a large number of actors from the public sector, the private sector and civil society developed a new phenomenon called Internet governance, based on a multi-stakeholder approach. The institutionalization of this process happened in 2005 when the United Nations Internet Governance Forum was set up. This thesis is analysing the process that built the multi-stakeholder Internet governance environment, with a focus on the two phenomenons cybercrime and Internet filtering.

SIGLAS

AoC – Affirmation of Commitments

APNIC – Asia-Pacific Network Information Centre

APWG – Anti-Phishing Working Group

ARIN – American Registry for Internet Numbers

ARPA – Advanced Research Projects Agency

ccTLD – Country Code Top Level Domain

DNS – Domain Name System

DOC – Department of Commerce

EFF – Electronic Frontier Foundation

gTLD – Generic Top Level Domain

IAB – Internet Architecture Board (before: Internet Advisory Board; Internet Activities Board)

IAHC – Interim Ad Hoc Committee (also: International Ad Hoc Committee)

IANA – Internet Assigned Numbers Authority

ICANN – Internet Corporation for Assigned Names and Numbers

ICCB – Internet Configuration Control Board

IETF – Internet Engineering Task Force

IFWP – International Forum on the White Paper

IGF – Internet Governance Forum

INHOPE – International Association of Internet Hotlines

INTA – International Trademark Association

IPTO – Information Processing Techniques Office

ISOC – Internet Society

ITU – International Telecommunication Union

JPA – Joint Project Agreement

MoU – Memorandum of Understanding

POC – Policy Oversight Committee

RIPE – Réseaux IP Européens Network Coordination Centre

TFFM – Task Force on Financial Mechanisms

WIPO – World Intellectual Property Organization

WGIG – Working Group on Internet Governance

WSIS – World Summit on the Information Society

FIGURAS

Figura 1: Localização dos Servidores Raiz em 2010 (p. 72)

Figura 2: Estrutura da ICANN (p. 97)

Figura 3: Mapa de Europa e Rússia (p. 127)

Figura 4: Mapa de Geórgia e Cáucaso (p. 131)

Figura 5: Padrão Web-Browsing (p. 161)

Figura 6: Filtragem TCP/IP (p. 164)

Figura 7: DNS Tampering (p. 166)

Figura 8: Filtragem HTTP Proxy (p. 169)

Figura 9: Green Dam (p. 182)

Figura 10: Filtragem na Internet e IDN ccTLDs (p. 192)

Figura 11: Liberdade de Imprensa e IDN ccTLDs (p. 192)

Figura 12: Págine de Bloqueio na Alemanha (p. 199)

TABELAS

Tabela 1: ONG Sub-Unidades (p. 45)

Tabela 2: Dez Princípios do Pacto Global das Nações Unidas (p. 57)

Tabela 3: Protocolo (p. 67)

Tabela 4: Operadores dos Servidores Raiz 2010 (p. 73)

Tabela 5: Modelo Trinomial de Controle da Internet (p. 173)

Tabela 6: Candidaturas a IDN ccTLDs (p. 191)

SUMÁRIO

Capítulo Um – Introdução.....11

1.1 Introdução Temática.....14
1.2 Estado de Conhecimento Científico.....17
1.3 Objetivo.....19
1.4 Relevância.....20
1.5 Perguntas de Pesquisa.....21
1.6 Metodologia.....23
1.7 Estrutura.....24

Capítulo Dois – Governança Global.....42

2.1 Governança Multisetorial.....53

Capítulo Três – Governança da Internet.....59

3.1 Introdução Histórica.....59
3.1.1 ARPA.....61
3.1.2 NPL.....63
3.1.3 RAND.....63
3.1.4 ARPANET.....65
3.1.5 Protocolos da Internet.....66
3.1.6 DNS.....69
3.1.7 IANA.....73
3.2 ISOC e o MoU.....75

3.3 ICANN.....83
3.3.1 Livro Verde.....83
3.3.2 Livro Branco.....90
3.3.3 Constituição da ICANN.....96
3.4 O Processo da ONU de WSIS ao IGF.....102

Capítulo Quatro – Crime Cibernético.....111

4.1 Raizes Históricas e Desenvolvimento do Crime Cibernético.....114
4.2 Stuxnet.....118
4.3 Dimensões Políticas do Crime Cibernético.....120
4.4 Crime Cibernético e Ataques Cibernéticos Políticos.....123
4.4.1 Rússia.....125
4.4.1.1 Estónia.....127
4.4.1.2 Geórgia.....131
4.4.2 China.....134
4.5 Atores Internacionais.....139
4.5.1 Conselho da Europa.....139
4.5.2 G8.....140
4.5.3 Nações Unidas.....142
4.5.3.1 União Internacional de Telecomunicações.....144
4.5.3.2 Outros.....145
4.6 Atores Regionais.....147
4.6.1 Cooperação Económica da Ásia e do Pacífico.....147
4.6.2 Comunidade das Nações.....148
4.6.3 União Europeia.....149
4.6.4 Organização dos Estados Americanos.....150
4.6.5 Organização para a Cooperação e Desenvolvimento Económico.....151
4.7 Sociedade Civil e Crime Cibernético.....153

Capítulo Cinco – Filtragem na Internet.....157

5.1 Métodos de Filtragem na Internet.....160
5.1.1 Método 1: Filtragem TCP/IP.....163
5.1.2 Método 2: DNS Tampering.....165
5.1.3 Método 3: Filtragem HTTP Proxy.....167
5.2 Filtragem na Internet em Países Não Democráticos.....171
5.2.1 China.....175
5.2.1.1 A Grande Firewall.....176
5.2.1.2 Blogs.....179
5.2.1.3 “Green Dam Youth Escort”.....180
5.2.1.4 Métodos de Circundamento.....183
5.2.1.5 Impacto Internacional da Filtragem na China.....183
5.2.2 Estratégias de Controle além de Filtragem.....184
5.2.2.1 Nomes Internacionais de Domínios.....187
5.3 Filtragem na Internet em Países Democráticos.....194
5.3.1 Pornografia Infantil.....197
5.3.2 O Debate Alemão sobre Filtragem na Internet.....198
5.3.2.1 Defensores e Oponentes.....200
5.3.3 Compartilhamento de Arquivos.....204

Capítulo Seis – Conclusão.....206

Bibliografia.....224

Capítulo Um: Introdução

No ano de 1980 o físico Britânico Tim Berners-Lee desenvolveu um programa de software que ele chamou de *Enquire*, baseado no título de um livro de auto-ajuda que havia encontrado na casa de seus pais quando criança "*Enquire within upon everything*". A idéia do *Enquire*, era facilitar seu trabalho diário com a criação de conexões virtuais entre pessoas e projetos diferentes no *European Particle Physics Laboratory* (CERN[1]), onde ele estava com um emprego provisório como consultor de *software*. Apenas Berners-Lee utilizava o programa *Enquire*, que ele desenvolveu em seu tempo livre. Apesar de ele ter deixado o *Enquire* para seus colegas quando seu tempo de trabalho na CERN terminou, a única cópia existente foi perdida. No entanto, a idéia básica desse pedaço de código de curta duração permaneceu na cabeça de Berners-Lee e o motivou a começar um projeto maior quando voltou a trabalhar na CERN em 1984. Sua idéia de desenvolver uma codificação que fosse capaz de facilitar a conexão entre computadores independente de sua localização física foi amplamente ignorada por seus superiores. Apesar de pesquisadores do EUA já estarem trabalhando com uma rede chamada ARPANET ou Internet, acadêmicos Europeus ignoravam essa nova tecnologia. Foi por esse motivo que a idéia de Berners-Lee de desenvolver um ambiente que permitiria que usuários se conectassem facilmente a outros computadores sem o uso de ordens complexas, como no caso da ARPANET, não encontrou muitos apoiadores. Depois de duas de suas propostas de pesquisa serem rejeitadas, ele decidiu mudar sua estratégia e reescrever seu projeto focando em um computador recentemente adquirido, chamado NeXT. Naquela época o NeXT, que havia sido apresentado em 1990 pela empresa homônima sob o co-fundador da Apple: Steve Jobs, havia entrado no mercado como a inovação de computadores pessoais e acabou nunca se tornando um produto comercial amplamente usado.

Para a realização de seu projeto Berners-Lee utilizou-se da idéia de links de hipertexto de Ted Nelson, que havia utilizado para o *Enquire* cerca de dez anos atrás.[2] Links de hipertexto foram um avanço lógico de referência, uma técnica fundamental para o trabalho acadêmico. Conectar-se a informações disponíveis em processos de qualquer computador do mundo, como acessar resultados de uma pesquisa publicada há muito tempo se possibiltou em segundos em vez de semanas ou meses. A linguagem de programação que Berner's Lee desenvolveu para seu objetivo se chamou

[1] CERN é a abreviação ao nome francês Conseil Européen por la Recherche Nucléaire.

[2] Ted Nelson é um sociologista dos EUA que desenvolveu em 1960 a idéia de hiperlinks e hipertextos que desenvolveu uma forma de desenvolver textos na qual o leitor pode decidir por si a hierarquia estrutural da leitura.

Hyptertext Markup Language (HTML) e se tornou a base para o primeiro browser chamado *WorldWideWeb*.[3] Como o projeto nunca foi inteiramente aceito pela CERN não há uma data específica para o dia em que ficou completo e que foi apresentado. Depois de meio ano de programação, em Março de 1991, Berners-Lee começou a distribuir o browser para seus colegas na CERN e em Maio para entidades de pesquisa dos EUA, que adaptaram o programa para o sistema de seus computadores.

O que nem Berners-Lee nem qualquer de seus colegas envolvidos no projeto poderiam ter imaginado naquela época era que a idéia que levou 10 anos do Enquête instalado apenas na empresa ao WorldWideWeb internacional teria um impacto significativo nos próximos 10 anos transcendendo o ambiente acadêmico ao acesso geral a informação e a uma série de outros setores da sociedade. Em sua primeira década de existência, o HTML se tornou a base para avanços em pesquisa e em educação, não apenas para instituições e organizações estabelecidas. Os primeiros passos foram dados para a conexão com áreas remotas e para providenciar educação áqueles que estavam em situações desavantajadas. Ao mesmo tempo os centros econômicos da economia mundial (especialmente os EUA) testemunharam o inicio do e-commerce e sua rápida propagação operando milhões de dólares todo mês. Grandes investimentos foram feitos na infra-estrutura da internet e o mercado de domínios demonstrou oportunidades de negociação que até então eram completamente desconhecidas. O desenvolvimento competitivo dessa nova economia resultou em grande crescimento do Mercado de ações e dentre alguns anos resultou em uma queda da economia.

Para a sociedade de atores civis, o HTML e a internet criou novas formas de participação política, arrecadação de fundos e relações publicas. Cidadãos que não conseguiam se organizar puderam trazer a tona seu comprometimento com a sociedade local e global. A introdução de páginas na web abriu portas a expressão publica de qualquer assunto possível, isso encaminhou a uma cultura mais compreensiva de informações individuais. Ao mesmo tempo, as páginas da web se tornaram um desafio para meios de comunicação tradicionais e para os governos, especialmente em estados autoritários. Foi esse o motivo que levou empresas e governos a buscarem maneiras de controlar o fluxo de informação que estava evoluindo. Enquanto isto, muitos jovens começaram a desenvolver novas tecnologias para expandir e melhorar o novo ambiente facilitando pesquisas e criando possibilidades para compartilhamento de arquivos com métodos alternativos ao download

[3] Observe a diferença entre o primeiro browser chamado WorldWideWeb e a World Wide Web (www) usada como uma expressão para a internet.

de um servidor. Essas novidades aceleraram a expansão da internet, criando novos modelos de negócios e ao mesmo tempo ameaçando os mercados tradicionais que dominavam no passado.

Passados mais 10 anos, a conectividade cresceu ainda mais e 30% da população mundial usava a Internet que era distribuída (heterogeneamente) para todas as partes do planeta. E os números ainda subiam. Novos grandes empreendimentos pela internet iniciaram uma competição pelos melhores modelos de negócio. Alguns começaram com redes temáticas na rede global tentando tornar perfeita a nova idéia de grupos de notícias. Nesse contexto, surgem novos desafios como a maneira de lidar com a questão da privacidade e da proteção de informações. A rede havia se expandido e todos os tipos de serviços se tornaram disponíveis on-line. Além disso, novos dispositivos foram desenvolvidos permitindo o uso de uma variedade de equipamentos para acessar a internet. Os governos em alguns países começaram a desenvolver os serviços públicos para seus cidadãos que estavam on-line. Alguns até transferiram processos de eleição para a internet. Outros intensificaram esforços para controlar atividades de seus cidadãos on-line.

Todas essas mudanças fizeram com que a segurança se tornasse uma questão central em níveis diferentes. Um deles era a segurança do usuário individual que havia se tornado um consumidor, que precisava de proteção contra fraudes e outras formas de pratica criminosa. Além disso, questões de segurança foram levadas a um nível mais amplo no qual diversas empresas estavam sofrendo ataques virtuais a suas redes diariamente

Mais adiante, estados se tornaram vítimas de ataques similares. Esses ataques podiam levar a um colapso temporário de sites representativos, a intrusões na infra-estrutura política e econômica que podiam se tornar muito sérias. Em alguns casos os governos se confrontavam com ataques virtuais em uma alta escala com força suficiente para derrubar a infra-estrutra critica de um país. Outros temiam tanto a influencia da internet sobre seu poder que decidiam desconectar todo o país em momentos estratégicos. E de fato, eles não estavam superestimando a situação. Em alguns casos a internet até contribuía para derrubar regimes autoritários.

Acompanhando todos esses avanços o caráter da pesquisa havia se modificado também. O que começou como uma rede para dar apoio a pesquisas de outros temas se tornou um objeto de pesquisa em si. Uma variedade de abordagens se disponibilizou, partindo das telecomunicações e

informática para o direito, estudos de comunicações e jornalismo, até a sociologia, ciências políticas e relações internacionais, entre outras. Pesquisas não envolviam apenas como a internet estava sendo usada, mas também em como seus usuários se comportavam on-line, como ela influenciava o pensamento das pessoas, como usuários começaram e mantiveram amizades e relacionamentos com pessoas que nunca haviam conhecido pessoalmente.. Estudos sobre como a rede e seus dispositivos influenciavam o status pessoal das pessoas, até mesmo *offline*, eram conduzidos. Além disso, pesquisadores começaram a analisar se e como a internet poderia levar ao vício e desconforto psicológico.

Perguntas sobre a interface da estrutura técnica, da administração, de questões legais e do ambiente político e social da internet se tornaram tópicos para pesquisa na área de Pesquisa de Governança da Internet. Pesquisa de Governança da Internet é uma área multidisciplinar de estudos na qual seus atores focam em vários problemas que são geralmente relatados ao processo de Governança da Internet das Nações Unidas (UN) institucionalizado no *Internet Governance Fórum* (Fórum de Governança da Internet) (IGF). O IGF foi estabelecido como um mecanismo de seguimento da World Summit on the Information Society (Cimeira Mundial Sobre a Sociedade da informação) (WSIS). O primeiro mandato da IGF aconteceu de 2006 a 2010. Paralelamente ao inicio do fórum a *Global Internet Governance Academic Network* (Rede Acadêmica de Governança da Internet Global) (GigaNet) foi fundada e promovia suas reuniões anuais junto a IGF. A GigaNet reflete a variedade de abordagens acadêmicas junto com a Comunidade de Governança da Internet. Como uma associação de pesquisa verdadeiramente multidisciplinar, ela abraça cientistas políticos e sociais, engenheiros, advogados e jornalistas, entre outros. Um aspecto essencial da pesquisa de governança da internet é a necessidade de conhecimento de questões técnicas relacionadas a redes e especialmente a internet. Isso se tornará obvio nessa tese que se utiliza de uma abordagem de relações internacionais e de ciências políticas mas também inclui uma série de detalhes técnicos originados pelas telecomunicações e informática. Outras abordagens (por exemplo estudos legais) não estão inclusas.

1.1 Introdução Temática

A primeira rede entre dois computadores foi desenvolvida em 1965 quando Lawrence Roberts do Instituto Tecnológcio de Massachusets (MIT) conectou dois computadores de Massachusets e Califórnia usando uma tecnologia de computação de pacotes (*packet switching*[4]) desenvolvida por Leonard Kleinrock (MIT) em 1961. A tecnologia anteriormente apenas de forma teórica por Kleinrock pode ser considerada a invenção subjacente para o que se tornou a Internet.Após o sucesso da rede de Robert, foram mais quatro anos até que mais computadores (em maior parte de instituições cientificas como a Universidade da Califórnia, Instituto de Pesquisa de Stanford, Universidade de Utah e mais tarde o MIT, Universidade de Harvard e mais) fossem adicionados. Naquele tempo, em 1969, a internet era conhecida como a ARPANET, desenvolvida pela ARPA, *Advanced Research Projects Agency*. A ARPA foi fundada em 1958 pelo departamento de defesa do EUA para promover desenvolvimento tecnológico depois do lançamento bem sucedido do satélite soviético *Sputnik* alguns meses antes. Portanto, a ARPANET por vezes é vista não somente como um meio de avanço da pesquisa cientifica civil e da comunicação, mas também como uma tecnologia com certo contexto (Giacomello 2005, p. 1). Nos anos procedentes ARPA (que depois também foi chamada de DARPA - *Defense Advanced Research Projects Agency* junto a pesquisadores de diversas universidades continuaram o desenvolvimento da ARPANET através do aprimoramento de padrões da Internet, protocolos (como o NCP, TCP/IP e o FTP) e outros componentes. Ao desenvolver o primeiro browser da internet no inicio de 1990 Tim Berners-Lee permitiu que a internet se tornasse uma ferramenta de uso público. Isso possibilitou que usuários privados fizessem parte da World Wide Web (WWW). A comercialização da internet e o crescimento de seu número de usuários levaram a questões organizacionais e de regulamentos em uma escala global. Um dos resultados desse debate foi a *International Corporation for Assigned Names and Numbers* (ICANN).

Falando em regulamento da internet e governança precisa-se distinguir entre dois tipos diferentes de definições do que deve ser governado.. Enquanto alguns cientistas se concentram em regulamentos técnicos e em questões institucionais quando falam em governança da internet, outros também levam em consideração aspectos relacionados a conteúdo para fazer parte da discussão

[4] Packet switching é a quebra de dados em datagramas ou pacotes que estão marcados para indicar a origem e o destino da informação e ao encaminhamento desses pacotes a partir de um computador a outro até que a informação alcance seu computador de destino final. Isso foi crucial para o alcance de uma rede de computadores. Se pacotes forem perdidos em qualquer momento dado, a mensagem pode ser reenviada pelo ponto de origem.

(Eijk; Maniadaki 2007, p. 67). Os próximos parágrafos vão concentrar primeiro em aspectos técnicos e depois no desenvolvimento e governança de conteúdo.

A condução de regulamentações técnicas da internet e sua infra-estrutura é feita em maior parte pela ICANN, que funcionou em 1988 como uma empresa sem fins lucrativos baseada na Califórnia. Nos anos antecedentes, atores diferentes como o *Internet Configuration Control Board* (ICCB) e o *Internet Advisory Board* (IAB) (que foi chamado depois de *Internet Activities Board* e depois *de Internet Architecture Board*) ou a *Internet Engineering Task Force* (IETF) junto a pessoas individuais se tornaram responsáveis pelas discussões de pesquisa e de política utilizando-se de informações de sistema horizontais como a *Request for Comments*[5] (RFC) ou pela criação do *Root Server System* ou o *Domain Name System*[6] (DNS). O DNS foi criado sem controle governamental e por muito tempo foi gerenciado por uma só pessoa: Jon Postel do Instituto de Informação Cientifica (ISI) na Universidade do Sul da Califórnia. Algumas das responsabilidades de Postel eram a delegação e a criação de domínios de topo genéricos (*generic top level domains*, gTLDs) como o .br, .de, ou .it. Ele por si delegava de domínios de topo de código de país (*country code top level domains*, ccTLDs) a pessoas em paises diferentes sem consultar o governo enquanto os três gTLDs mencionados eram gerenciados pela empresa privada *Network Solutions Inc*. (NSI). Em 1988 Postel fundou a *Internet Assigned Numbers Authority* (IANA) dentre o ISI para a estabilização e institucionalização técnica de regulamentação da internet. O ISI por si foi contratado pelo Departamento de Comércio Americano (*Department of Commerce*, DOC) para a manutenção do controle do DNS ou de funções regulatórias.

Com a criação do WWW Jon Postel (e outros) decidiu que iria criar um número maior de gTLDs para possibilitar que usuários privados e comerciais se utilizassem da Internet. Como isso exigia um esforço organizacional e administrativo muito maior Postel chegou a conclusão de que era necessário um quadro institucional diferente para o DNS. Sua idéia era usar a *Internet Society* (ISOC[7]) como autoridade responsável.

[5] RFCs são memorandos e notas de pesquisa distribuídos inicialmente pelo correio original e posteriormente pelo acesso eletrônico.

[6] A DNS é uma rede hierárquica internacional de nomes de servidores que possibilitam a comunicação entre computadores.

[7] A ISOC foi fundada em 1992 como uma organização não governamental representando a comunidade da internet.

Nem o governo do EUA nem a Network Solutions apoiaram sua idéia da criação de TLDs e de entregar o DNS para a ISOC. Em 1996 Postel estabeleceu o *Interim Ad Hoc Committee* (IAHC) que considerou membros da ISOC, da IANA, da IAB, a *International Telecommunication Union* (ITU), a *International Trademark Association* (INTA) e a *World Intellectual Property Organization* (WIPO). As duas últimas foram criadas para lidar com uma preocupação crescente de uso indevido de marcas registradas na Internet.

Em Maio de 1997 a IAHC assinou um memorando de compreensão (gTDL-MoU). Com base no memorando o *Policy Oversight Committee* (POC) foi formado e posteriormente criou um número limitado de TLDs. Mais uma vez, todo o processo foi criticado pela administração do EUA, que sob o poder do presidente Clinton iniciou seus próprios esforços para privatização do DNS. Postel também se envolveu no processo e em Novembro de 1998 a ICANN foi finalmente estabelecida e um memorando foi fechado entre a ICANN e o DOC. Dessa maneira a administração dos EUA tentava manter o controle do regulamento da internet. O memorando originalmente ia ser estabelecido por dois anos, após os quais a ICANN se tornaria independente da influencia governamental dos EUA. Houve uma alteração nessa decisão e após dois anos foi formada um novo memorando, seguido pelo *Joint Project Agreement* (JPA). Além do JPA a ICANN e as partes da administração dos EUA tinham mais três contratos.

As principais funções da ICANN foram estabelecidas para envolver os regulamentos técnicos da internet. Entretanto, com o passar dos anos de sua existência tornou-se claro que a internet tinha mais do que apenas um lado técnico. Essa impressão se fortaleceu entre atores envolvidos em debates globais sobre a sociedade da informação e a internet, especialmente durante o *World Summit on the Information Society* (WSIS, 2033-2005) quando um grande número de atores de países e histórias diferentes se reuniram para a discussão de benefícios e desafios globais de tecnologias da informação e da comunicação (ICT). Nesse contexto o foco era levantar um número de tópicos políticos e sociais como o uso de ICTs para desenvolvimento econômico, liberdade de expressão ou empoderamento de pessoas que viviam em áreas rurais. Durante o WSIS ficou claro que havia necessidade de criar um debate continuo sobre a internet que foi desenvolvido com o estabelecimento do Fórum de Governança da Internet (*Internet Governance Forum*, IGF). O IGF encontrou pela primeira vez em 2006 e nos próximos anos expandiu seu foco para uma variedade de questões relacionadas à internet. Dois desses focos serão analisados nessa tese, sendo o crime

cibernético (dentro do contexto de segurança cibernética) e a filtragem na internet. Os dois são os tópicos mais desafiadores da governança da internet do momento. E a filtragem na internet está se destacando entre os tópicos da agenda internacional em relação a políticas da internet.

1.2 Estado de Conhecimento Científico

Depois de Tim Berners-Lee ter desenvolvido o primeiro browser em 1991 a pesquisa política sobre a internet teve um inicio lento como uma nova abordagem até que se tornou mais visível por volta dos anos 1990. Havia um pequeno número de cientistas que focavam em certos aspectos políticos da internet como no *Visions of Governance for the Twenty-first Century Project* fundado em 1996 na John F. Kennedy School of Governance em Harvard. Lá, Joseph Nye e outros pesquisadores e estudantes investigavam os efeitos das novas tecnologias de informação e de comunicação (sigla em inglês: NICT) sendo desenvolvimento, participação política, campanhas eleitorais e possibilidades de democracia virtual (Nye; Kamarck 2002). Ao mesmo tempo Michael Mazarr publicou o livro *Information Technology and World Politics* no qual um número de cientistas apresentavam pesquisas de estudos de caso em TIC e política de segurança na Índia, no Brasil, no Peru e na China (Mazarr 2002).

Além desses dois Juliann Emmons Allison também estudou questões relacionadas ao WWW. Perguntando a si mesma se as TICs tinham alguma conseqüência em relações internacionais ela desenvolveu um modelo de três abordagens diferentes: a resposta neutra, a resposta positiva e a reposta crítica (Allison 2002, p. 5ff). Segundo a abordagem da resposta neutra, inovação na área de tecnologia da informação é um fenômeno de desenvolvimento contemporâneo assim como foram os telefones e as maquinas de lavar roupa. Portanto as TIC têm se tornado parte da politica internacional, mas não a influenciam ou a mudam. A abordagem da resposta positiva expressa que as TICs têm alto impacto nos atores políticos e portanto influenciam seus comportamentos e decisões. A terceira abordagem (resposta crítica) se refere ao fato de que o acesso às TICs é limitado em uma escala global e ocorre principalmente em países industrializados e em menor escala em países recentemente industrializados e em desenvolvimento. Muitos estudos de desenvolvimento seguem essa abordagem, lidando com a exclusão digital e outros tópicos de

desenvolvimento.

As publicações mencionadas não podem ser consideradas como pertencentes a uma área de pesquisa específica da internet. A maioria foi escrita dentro de uma estrutura de assuntos clássicos de relações internacionais (por exemplo desenvolvimento ou estudos de segurança). Também não há conexões diretas entre publicações como *The Internet Galaxy* (Castells 2001*), Open Networks, Closed Regimes* (Kalathil; Boas 2003) ou *The Politics of Internet in Third World Development* (Hoffmann 2004).

No entanto, no caso da governança da internet podemos citar claramente um campo de pesquisa em evolução. Há um número crescente, mas no entanto ainda pequeno de monografias, antologias e uma seleção de artigos científicos e literatura cinzenta lidando com a regulamentação da internet, ICANN, o IGF e campos diferentes de política da internet. Uma razão para isso é o debate e o processo continuo sobre a ICANN, o WSIS e o IGF. Outra é a fundação da GigaNet que deu a pesquisa sobre a governança da internet uma base institucional.

Ruling the Root de Milton Muellers pode ser considerada uma monografia central para o entendimento de técnicas básicas da internet e governança da internet. Mueller, Wolfgang Kleinwächter, Hans Klein e William Drake são alguns dos pesquisadores que se envolveram em estudos da governança da internet por muitos anos. Eles (e outros) tem feito publicações de processos de governança da internet e regulamentação técnica de uma perspectiva de governance global. Algumas publicações recentes são *Internet Governance in a Global Multi-Stakeholder Environment* (Kleinwächter 2007), *The Internet and Global Governance: Principles and Norms for a New Regime* (Mueller; Mathiason; Klein 2007), *Internet Governance and the Information Society: Global Perspectives and European Dimensions* (Benedek; Bauer; Kettemann 2008), *Governing the Internet: The Emergence of an International Regime* (Franda 2001), *Multi-Stakeholder Governance and the Internet Governance Forum* (Malcolm 2008) e *Networks and States* (Mueller 2010). Essas abordagens gerais de estruturas de governança da internet oferecem os princípios básicos para a compreensão do quadro maior e contexto histórico por trás da pesquisa de governança da internet. Para essa tese elas são uma parte importante da literatura fundamental.

1.3 Objetivo

O objetivo dessa tese é contribuir a área de pesquisa interdisciplinar relativamente nova de governança da internet de uma perspectiva de relações internacionais. O autor pretende analisar as oportunidades e os limites dos processos de governança multisetorial. Haverá um foco nos dois sub-campos de filtragem na internet e de crimes cibernéticos para descobrir a maneira como grupos de interesse e atores diferentes estão participando e cooperando nessas áreas e como isso afeta o processo de governança da internet em geral.

O processo de governança da internet é baseado em uma abordagem multisetorial como foi destacado no relatório de 2005 do *Working Group on Internet Governance* (WGIG) e na *Tunis Agenda* que foi desenvolvida durante o *World Summit on the Information Society*. Se torna obvio, ao comparar a governança da internet com outros processos de governança global, que a abordagem multisetorial não está dominando a área de pesquisa sobre governança global. De fato, há poucos exemplos de processos multisetoriais, enquanto na maior parte dos casos os governos são os únicos atores (mesmo que estes as vezes incluam participantes selecionados de outros grupos de interesse). Atores em um ambiente multisetorial como o IGF vêm do setor publico, do setor privado e da sociedade civil. Aqui se torna claro em como essa abordagem pode distinguir da governança privada onde são consideradas parte do setor privado ambas empresas privadas e a sociedade civil. (Pattberg, 2004, p12f). Nos processos de governança multisetorial não só cresce o número de atores, mas também há uma diversidade maior de interesses nos assuntos de governança. No caso de filtragem na internet isso se esclarece especialmente ao observar as organizações de direitos humanos por um lado e interesses econômicos de empresas de TI por outro lado. Além disso os governos em países filtrando a internet (por exemplo a China) consideram isso seu direito soberano como controle de conteúdo.

Enquanto o problema da filtragem demonstra uma diversidade de pontos de vista dos atores involvidos que dificilmente se ajustam um ao outro, os crimes cibernéticos apresentam outro desafio. Existem formas variadas de crime cibernético como hacking, phishing, ataques de negação de serviços, spams e outros. Alguns deles têm um contexto econômico e outros têm um contexto político. Em muitos casos, o crime cibernético é cometido além dos limites de fronteira nacional, que não só torna difícil saber quem é o infrator, mas confronta as forças policiais nacionais com o

problema de que a soberania está limitada ás fronteiras nacionais. Além disso, atos cometidos em um país em que estão dentro da lei podem ser considerados um crime em outro país devido ás diferenças de seus sistemas jurídicos. Um exemplo é um conflito que há entre a liberdade de expressão nos EUA e a discriminação racial em diferentes países europeus. Em outros casos, a falta de uma legislação adequada sobre as atividades on-line pode ajudar certas pessoas a cometerem crimes em outros países pela internet. O crime cibernético pode até mesmo gerar tensões entre países como é o caso da China e da Alemanha e dos EUA e do Reino Unido. (Sueddeutsche.de 2007b; Spiegel Online 2007a; Spiegel Online 2007b). A China foi culpada por ataques cibernéticos a instituições públicas diferentes pelos outros três países em 2007. Enquanto nesses casos os atacantes pareciam agir de instituições governamentais da China, as tensões entre a Rússia e a Estónia decorrentes de ataques cibernéticos no mesmo ano foram, obviamente, causadas por cidadãos particulares (Kirk 2008). Já em 2001 a União Européia apresentou uma convenção sobre o crime cibernético..Mas até hoje seus efeitos são assuntos de uma discussão controversa.

1.4 Relevância

Em 2002 Mazarr explicou em *Information Technology and World Politics*:

> This volume examines a subject that has so far received scant attention, at least in terms of formal, rigorous research projects: the effect of information technology on world politics, and specifically the growing role of the Internet in promoting freedom and changing social and political norms. (Mazarr 2002, p. 1).

Até 2010 o número de projetos de pesquisa envolvendo política e a internet têm aumentado, mas pode-se repetir a frase sobre a falta de atenção em relação aos estudos de governança da internet destacando abordagens de relações internacionais. Como citado anteriormente, houve um número pequeno (mas crescente) de projetos de pesquisa acadêmica e de publicações desde que a WGIG desenvolveu a primeira definição de governança da internet em 2005. No entanto, poucos desses projetos se utilizam de uma abordagem de ciência política e quase nenhum vem da área de relações

internacionais. No entanto, o quadro teórico de relações internacionais oferece uma variedade de oportunidades para a inclusão desse assunto em sua área de estudos. Isto não se refere apenas a área de governança global utilizada nessa tese, mas também a analise de conflitos internacionais, organizações internacionais, estudos de desenvolvimento e construção de regimes para citar alguns.

A internet não é um fenômeno passageiro, mas uma tecnologia que irá permanecer e que já está dominando grande parte da vida dos cidadãos, empresas e governos. O crime cibernético e a filtragem na internet também têm uma relevância crescente. O caráter não-territorial da internet desfavorece soluções nacionais e por esse motivo o processo de governança da internet têm acontecido a nível internacional. De qualquer maneira, também há governos que se manifestam em termos de soluções a nível nacional. O conflito entre esses dois modelos básicos apenas começou o que destaca a relevância da analise de detalhes deste debate de uma perspectiva de relações internacionais.

1.5 Perguntas de Pesquisa

A pergunta de pesquisa central é:

Como o ambiente multisetorial na governança da internet afeta os fenômenos de crime cibernético e de filtragem na internet?

Há um número de sub-perguntas que devem ser consideradas também:

a) Como o processo de governança multisetorial se desenvolveu no passado?

b) Quais atores estão envolvidos no processo de governança da internet?

c) Quais os interesses de atores diferentes em relação a crime cibernético e a filtragem na internet?

d) Como os atores atuam nos campos de crime cibernético e de filtragem na internet?

e) Como os atores diferentes cooperam ou bloqueiam umas as outras?

f) Como a cooperação ou não-cooperação entre atores diferentes afetam o processo de governança do crime cibernético e da filtragem na internet?

g) Quais são as conclusões que podem ser tiradas em relação à abordagem de governança multisetorial baseadas em uma analise dos campos do crime cibernético e da filtragem na internet?

Hipóteses:

a) O caráter de discussão aberta providenciado pelo Fórum de Governança da Internet encaminhará a uma troca de idéias produtivas usadas por todos os atores. No entanto, dificilmente haverá um contrato ou se chegará a um consenso entre todos os atores devido a divergência dificilmente combinável de interesses. Ao invés, haverá numerosos acordos parciais entre as partes interessadas.

b) Apesar de todos os atores terem interesses divergentes, as diferenças entre o setor privado e o setor governamental (especialmente no caso de filtragem na internet) serão resolvidas com maior facilidade do que entre atores da sociedade civil e os outros dois grupos de atores.

c) No caso do crime cibernético os atores terão mais facilidade em entrar em um acordo do que no caso da filtragem na internet, já que o primeiro é considerado uma ameaça virtual a todas as partes enquanto que o segundo é visto como uma questão de soberania e interesses financeiros contra direitos humanos e democráticos.

d) Ha uma possível relação entre o crime cibernético e a filtragem na internet. Um aumento de atividades de crime cibernético pode levar a um grau mais alto de filtragem na internet. Uma proteção internacional efetiva contra o crime cibernético pode resultar em uma redução da filtragem na internet.

e) Sem convenções internacionais o crime cibernético resultará em uma limitação de direitos básicos (e direitos humanos) em estados autoritários tanto quanto em estados democráticos.

1.6 Metodologia

Esta tese é desenvolvida utilizando-se a metodologia de pesquisa qualitativa de estudo de caso. “Um estudo de caso (...) é a analise de um objeto: um país, um sistema político, uma instituição, uma organização, ou um problema inserido em um contexto específico (...). Em uma analise comparativa são utilizados casos diferentes sobre um mesmo assunto.” (Nohlen 1994, p. 128, *tradução pelo autor*). O estudo de caso é um dos métodos mais aplicados em pesquisa política. Sua origem vai a 1948 a Universidade de Harvard (McNabb 2004, p. 357). Ele ajuda a explicar casos específicos e também possibilita a formação de generalizações (apesar de métodos quantitativos serem mais fortes para as generalizações). Pode ser conduzido usando um ou vários casos. “Através do estudo de casos cientistas políticos podem aprender sobre eventos políticos, agencias, partidos e níveis de governo e política ao redor do mundo.” (idem).

Robert Stake (1994, p. 237) divide estudos de casos em três categorias: intrínseco, instrumental e estudos de casos coletivos. Desta forma, ele tenta diferenciar os motivos dos pesquisadores. Um estudo intrínseco visa a compreensão do caso em si. O caso é o aspecto central do estudo. O objetivo não é nem desenvolver teorias e nem analisar fenômenos por trás de um caso. Um estudo instrumental trata o caso como um exemplo para a formulação de uma teoria ou de um fenômenos social ou político. Esse fenômeno é que vem ao interesse do pesquisador. O caso pode ajudar a explica-lo. A terceira categoria é o estudo de caso coletivo. O pesquisador o utiliza para investigar vários casos que ajudam a explicar um fenômeno específico. Semelhante a Stake, Robert Yin divide os estudos de caso em duas categorias: estudos de casos únicos e estudos de casos múltiplos (Yin 2003, p. 39ff). Ambos tem como intenção a explicação de um fenômeno por trás do caso. John Gerring inclui unidades de analise em sua definição de estudo de caso. Portanto, ele define um estudo de caso como “an intensive study of a single unit for the purpose of understanding a larger class of (similar) units” (Gerring 2004, p. 342).

Essa tese vem analisar o ambiente multisetorial no processo de governança da internet com foco especial nos dois casos de crime cibernético e filtragem na internet. É um estudo de casos múltiplos que vai ajudar a a) analisar fenômenos de crimes cibernéticos e filtragem na internet, b) analisar atores diferentes envolvidos no processo de governança da internet e suas relações uns com os outros, c) fazer afirmações gerais sobre a governança da internet e processos de governança

multisetorial.

Os quatro tipos de fontes de evidência seguintes foram utilizados:

1) **analise de documento:** literatura cientifica, artigos de jornal, documentos e literatura cinzenta publicados por atores diferentes e durante reuniões institucionalizadas como WSIS, IGF e outras.

2) **observação direta:** observação de reuniões dos atores no IGF e online (algumas reuniões dos atores ou instituições como a ICANN são transmitidas online na internet).

3) **entrevistas não estruturadas:** conversas e entrevistas com participantes do IGF e outros envolvidos no processo de governança da internet.

4) **entrevistas estruturadas:** questionários detalhados desenvolvidos para juntar informações específicas de pesquisadores e especialistas envolvidos no processo de governança da internet.

1.7 Estrutura

A estrutura da tese consiste nesta introdução (capítulo um), quarto partes temáticas (capítulos 2 a 5) e a conclusão (capítulo seis).

O segundo capítulo concentra-se em dois fenômenos de governança global e governança multisetorial. Lá dentro, uma analise atual sobre os dois conceitos teóricos é conduzida. A governança multisetorial será inserida em um contexto histórico e conceitual. Além disso, será discutido os motives e a maneira em que ambientes multisetoriais tem se desenvolvido nos últimos anos.

O terceiro capítulo concentra-se no processo de governança da internet. Ele inclui uma introdução histórica das origens e do desenvolvimento da internet. Neste contexto também sera mencionada a funcionalidade técnica que é importante para a compreensão dos detalhes dos estudos de caso

seguintes. Além disso, os atores principais são discutidos nesse capítulo, entre eles IANA e ICANN, tanto quanto o processo da ONU incluindo o WSIS, o WGIG e o IGF.

O quarto capítulo inclui o primeiro estudo de caso com foco no crime cibernético. Nesse sentido o crime cibernético é explicado em um quadro mais amplo de segurança cibernética incluindo outras formas de questões de segurança como a guerra cibernética e ataques cibernéticos em geral. É importante a compreensão da relação entre categorias diferentes já que a maioria dos ataques cibernéticos esta relacionada de alguma forma ao crime cibernético não importando se estão inseridos em um contexto político ou econômico. As relações entre o crime cibernético ordinário ou ataques cibernéticos com motivações políticas se tornam aparentes ao avaliar exemplos de conflitos cibernéticos envolvendo a Rússia, a Estónia, a Geórgia e também a China. Além disso, haverá um foco em organizações regionais e internacionais assim como a sociedade civil.

O capítulo cinco é o segundo estudo de caso e lida com problemas de filtragem na internet. Para a compreensão desse fenômeno é necessário recordar a funcionalidade técnica da internet dada no capítulo três. Também é necessário entender os métodos técnicos usados para manipular o fluxo livre de informação online. Por essa razão, os métodos centrais de filtragem da internet serão discutidos. Além disso, um número de modelos didáticos será incluso para explicar os motives e as maneiras da filtragem na internet pelos governos. A idéia desse modelos é dar apoio à argumentação do estudo de caso, mas também podem ser aplicados em outros contextos. Por exemplo em aulas de relações internacionais que lidam com a filtragem na internet como uma questão de política internacional. Depois disso, serão discutidos processos de filtragem em países não democráticos e democráticos. Será enfatizado o sistema chinês de filtragem (está entre os mais sofisticados atualmente) e o debate Europeu sobre filtragem na internet, especialmente na Alemanha.

No último capítulo os resultados do estudo serão utilizados para desenvolver conclusões finais sobre assuntos específicos da tese e sobre o projeto de pesquisa em geral.

Chapter One: Introduction

In the year 1980 the British physicist Tim Berners-Lee developed a software program which he called Enquire, based on the title of a self-help book he had found in his parent's home as a child ("Enquire within upon everything"). The idea of Enquire was to facilitate his daily work by creating virtual connections between different people and projects at the European Particle Physics Laboratory (CERN[8]) where he was staying for a temporary job as a software consultant. Enquire, which he wrote in his free time, was only used by Berners-Lee himself and although he passed it on to his colleagues after his job at the CERN was finished, the only existing copy got lost. Nevertheless, the basic idea of this short-lived piece of code remained in Berners-Lee's head and motivated him to start a larger project when he went back to work at CERN in 1984. His idea to develop a code that was able to facilitate the connection between computers independently of their physical location was widely ignored by his superiors. Although researchers in the U.S. were already working with a network called ARPANET or the Internet, European academics widely ignored this new technology. For this reason Berners-Lee's idea to develop an environment which would enable users to easily connect to other computers without using complex orders as it was the case for the ARPANET did not find a lot of supporters. After two of his research proposals were disregarded he decided to change his strategy and rewrote his project turning its focus to a newly acquired computer called the NeXT. At that time the NeXT, which was presented in 1990 by the homonymous company under Apple co-founder Steve Jobs, had entered the market as a groundbreaking personal computer but which in the end never became a widely used commercial product.

To realize his project, Berners-Lee picked up the idea of Ted Nelson's hypertext links that he had used for the Enquire about ten years before.[9] Hypertext links were the logical advancement of referencing, a fundamental technique of academic work. By connecting information available on any computer in the world processes like accessing necessary research data published in a far distance were realizable in seconds instead of weeks or months. The programing language Berners-Lee had developed to realize his plan was named Hyptertext Markup Language (HTML) and became the basis for his first browser called WorldWideWeb[10]. As the whole project was never

[8] CERN is the abbreviation for the French name Conseil Européen por la Recherche Nucléaire.

[9] Ted Nelson is a U.S. sociologist who in the 1960s developed the idea of hyperlinks and hypertext to describe a way of developing texts in which the reader himself could decide about the structural hierarchy of reading.

[10] Note the difference between the first browser called WorldWideWeb and the World Wide Web (www) as an

officially accepted by CERN there is no fixed date when it was completed or presented. After half a year of programing, in March 1991 Berners-Lee started distributing the browser among his colleagues at CERN and in May also at research entities in the U.S. which adapted it to their own computer systems.

What neither Berners-Lee nor any of his colleagues involved in the project would have imagined at that time was that the idea that took about ten years from the locally installed Enquire to the internationally usable WorldWideWeb browser would within another 10 years have a major impact not only on the academic environment and general access to information but also on a number of other sectors of society. In the first decade of its existence HTML became the basis for advances in research and education and not just for established institutions and organizations. Also the first steps were taken to connect remote areas and to provide education to those that had been living in disadvantaged situations over years and decades. At the same time the economic centers of the world economy (and especially the U.S.) witnessed the start and a rapid boost of e-commerce transacting millions of U.S. dollars every month. Large investments were made also in the infrastructure of the Internet and the domain name market opened business opportunities which by that time had been completely unknown. The racy development of this new economy also lead to a boom on the stock market and after a few years resulted in an economic downfall.

For civil society actors HTML and the Internet created new forms of political participation, fund-raising and public relations and also individual and unorganized citizens were able to bring forward their commitment to their local or global society. The introduction of weblogs opened up the door to publicly speaking out about any topic possible, which lead to a more comprehensive culture of individual information. At the same time weblogs became a challenge for traditional media outlets and governments especially in authoritarian states. For this reason the first companies and governments started thinking about how to control the just evolving free flow of information. Meanwhile, mostly young people started developing new technologies to expand and improve the new environment by making it search-able or by creating possibilities to share files in different manners than just downloading them from a server. These new inventions accelerated the expansion of the Internet, created new business models and at the same time threatened or undermined those that had dominated traditional markets in the past.

expression for the Internet.

Another 10 years later connectivity had increased further and 30% of the world population was using the Internet, distributed (unequally) over all parts of the planet. And numbers were still increasing. New large Internet enterprises had come up and started competing for the best business models. Some started creating thematic networks within the global network trying to bring the early idea of newsgroups to perfection. In this context new challenges came up like the question for privacy and data protection. The network had expanded and all kinds of services became available online. Besides that new devices had been developed allowing to access the Internet using a variety of equipment. Governments in some countries had started improving public services for its citizens online. Some even transferred election processes to the Internet. Others intensified their efforts to control online activities of their citizens.

All of these changes let security become a central issue on different levels. One of them was security of the individual user who had become a customer needing protection against fraud and other forms of criminal practices. Besides that, questions of security had also been taken onto a broader level in which several companies were suffering virtual attacks on their networks on a daily basis. Furthermore, states had become victims of similar attacks. These attacks could lead from a temporary breakdown of representative websites to serious intrusions into political or economical infrastructure. In some cases governments saw themselves confronted with virtual attacks on a large scale with enough force to bring down a country's critical infrastructure. Others feared the influence of the Internet on their own power so much that they decided to disconnect the whole country at strategic moments. And in fact they did not overestimate the situation. In some cases the Internet even contributed to overthrow authoritarian regimes.

Along with all these developments also the research character of the Internet had changed. What started as a network to support research on other topics became an object of research itself. A variety of approaches came into being, ranging from telecommunications and informatics over law, media studies and journalism until sociology, political science and international relations among others. Research was done not only on how the network could be technically improved but also how its users behaved online, how it influenced people's thinking, how users started and maintained friendships and relations with people they had never met in person. Studies were conducted on the question how networks and devices influenced people's social status even in the offline world. Besides that, researchers started analyzing if and how the Internet could lead to psychological

uneasiness and addiction.

Also questions regarding the interface of technical structure, administration, legal issues and the political and social environment of the Internet became research topics that were merged in the area of Internet governance research. Internet governance research is a multi-disciplinary area of studies whose actors focus on various problems which are often related to the Internet governance process of the United Nations (UN) institutionalized in the Internet Governance Forum (IGF). The IGF was established as a follow-up mechanism of the World Summit on the Information Society (WSIS). The first IGF mandate happened between 2006 and 2010. Parallel to the start of the forum the Global Internet Governance Academic Network (GigaNet) was founded which held its annual meetings together with the IGF. GigaNet reflects the variety of academic approaches within the Internet governance community. As a truly multi-disciplinary research association it embraces political and social scientists and engineers as well as lawyers and journalists among others. An essential aspect of Internet governance research is the necessary knowledge of technical issues related to networks and especially to the Internet. This will become obvious in this thesis which uses an international relations and political science approach but also includes a number of technical details originating from telecommunications and informatics. Other approaches (e.g. legal studies) are not included.

1.1 Thematic Introduction

The first network between two computers was set up in 1965 when Lawrence Roberts of the Massachusetts Institute of Technology (MIT) connected two computers in Massachusetts and California using packet switching technology[11] developed by Leonard Kleinrock (MIT) in 1961. Kleinrock's formerly only theoretically developed technology can be considered to be the underlying invention for what later became the Internet. It took another four years after the success of Roberts' network until more computers (mostly from scientific institutions like the University of California, Stanford Research Institute, University of Utah and later the MIT, Harvard University

[11] Packet switching is the breaking down of data into datagrams or packets that are labeled to indicate the origin and the destination of the information and the forwarding of these packets from one computer to another computer until the information arrives at its final destination computer. This was crucial to the realization of a computer network. If packets are lost at any given point, the message can be resent by the originator.

and more) were added. At that time in 1969 the Internet was known as ARPANET, developed by ARPA, the Advanced Research Projects Agency. ARPA was originally founded in 1958 by the U.S. Department of Defense to foster technological development after the successful launch of the soviet satellite Sputnik a few months before. Therefore, the ARPANET is sometimes not only seen as a means to improve civil scientific research and communication but also as a technology with a certain military background (Giacomello 2005, p. 1). In the following years ARPA (later also called DARPA – Defense Advanced Research Projects Agency) together with researchers from different universities continued to improve ARPANET by developing Internet standards, protocols (like NCP, TCP/IP and FTP) and other components. By developing the first Internet browser in the beginning of the 1990s Tim Berners-Lee opened up the Internet for public use. This enabled private users to participate in the World Wide Web (WWW). The commercialization of the Internet and the growth of user numbers lead to the question of organization and regulation on a global scale. One of the results of this debate was the International Corporation for Assigned Names and Numbers (ICANN).

Talking about Internet regulation and governance it needs to be distinguished between two different types or definitions of what has to be governed. While some scientists concentrate on technical regulations or institutional issues when they talk about Internet governance others also consider content related aspects to be part of the discussion (Eijk; Maniadaki 2007, p. 67). The following paragraphs will concentrate first on the technical aspects and then on development aspects and the governance of content.

Technical regulation of the Internet and its infrastructure is mainly conducted by ICANN which was founded in 1998 as a California-based non-profit-organization. In the years before, different actors like the Internet Configuration Control Board (ICCB) and the Internet Advisory Board (IAB) (which was later called Internet Activities Board and later Internet Architecture Board) or the Internet Engineering Task Force (IETF) together with individual persons were responsible for policy and research discussions by using horizontal information systems like the Request for Comments[12] (RFC) or for creating the Root Server System or the Domain Name System (DNS[13]). The DNS was created without any governmental control and for a long time managed by a single

[12] RFCs are memos and research notes originally distributed by traditional mail and later by electronic access.

[13] The DNS is a worldwide hierarchical net of name servers to enable communication between computers.

person: Jon Postel of the Information Science Institute (ISI) at the University of Southern California. Some of Postel's responsibilities were the creation and delegation of generic top level domains (gTLDs) like .com, .org, and .net as well as country code top level domains (ccTLDs) like .br, .de or .it. He himself delegated ccTLDs to people in different countries without any governmental consultations while the three mentioned gTLDs were managed by the private company Network Solutions Inc. (NSI). In 1988 Postel founded the Internet Assigned Numbers Authority (IANA) within the ISI to stabilize and to institutionalize technical Internet regulation. The ISI itself was contracted by the U.S. Department of Commerce (DOC) to maintain control over the DNS and other regulatory functions.

With the invention of the WWW Jon Postel (and others) decided to create a bigger number of gTLDs to enable private and commercial users to participated in the Internet. As this would have meant a much higher organizational and administrative effort Postel came to the conclusion that a different institutional framework for the DNS was needed. His idea was to use the Internet Society (ISOC)[14] as a responsible authority. Neither the U.S. government nor Network Solutions supported his decision to create new TLDs and to hand over the DNS to ISOC. In 1996 Postel established the Interim Ad Hoc Committee (IAHC) which consisted of members from ISOC, IANA, IAB, the International Telecommunication Union (ITU), the International Trademark Association (INTA) and the World Intellectual Property Organization (WIPO). The last two mentioned were invited to take care of the growing concern about misuse of registered trademarks on the Internet.

In May 1997 IAHC signed a Memorandum of Understanding (gTLD-MoU). Based on the memorandum the Policy Oversight Committee (POC) was formed which later decided to create a limited number of new TLDs. Again the whole process was criticized by the U.S. Administration which under President Clinton started its own efforts to privatize the DNS. Also Postel became involved in that process and in November 1998 ICANN was finally established and a MoU was set up between ICANN and the DOC. By this way the U.S. Administration tried not to loose control over the regulation of the Internet. The MoU was originally set up for two years after which ICANN should become independent from U.S.-governmental influence. This decision was altered and after two years a new MoU was formulated, later followed by the Joint Project Agreement (JPA). Besides the JPA there were three more contracts between ICANN and different parts of the U.S.-

[14] ISOC was founded in 1992 as a non-governmental organization representing the Internet community.

administration.

ICANN's main tasks were set to be the technical regulation of the Internet. However, within the first years of its existence it became clear that there was more than a technical side to the Internet. This impression became stronger among the actors involved in global debates on the information society and the Internet, especially during the World Summit on the Information Society (WSIS, 2003-2005) when a huge number of actors from different countries and backgrounds met to discuss global benefits and challenges of information and communication technologies (ICT). In this context the focus was put on a number of political and social topics like the use of ICTs for economical development, freedom of expression or empowerment of people living in rural areas. During the WSIS it became clear that there was a need to create an ongoing debate on the Internet which was achieved by establishing the Internet Governance Forum (IGF). The IGF met for the first time in 2006 and by the years expanded its focus on a variety of issues related to the Internet. Two of them will be analyzed in this thesis, being cybercrime (within the cybersecurity context) and Internet filtering. Both are among the most challenging topics of Internet governance at the time. And especially Internet filtering is among the latest topics of the international agenda concerning Internet politics.

1.2 State of Scientific Knowledge

After Tim Berners-Lee had developed the first browser in 1991 political research on the Internet started out slowly as a new approach until it became more visible in the mid 1990s. There was a small number of scientists who focused on certain political aspects of the Internet like in the *Visions of Governance for the Twenty-first Century Project* founded in 1996 at the John F. Kennedy School of Governance at Harvard. There, Joseph Nye and other researchers and students were investigating the effects of new information and communication technologies (NICT) on development, political participation, electoral campaigns and the possibilities of cyberdemocracy (Nye; Kamarck 2002). At the same time Michael Mazarr published the book *Information Technology and World Politics* in which a number of scientists presented case study research on ICT and security politics in India, Brazil, Peru and China (Mazarr 2002).

Besides these two also Juliann Emmons Allison studied questions related to the WWW. Asking herself if ICTs had any consequence on international relations she developed a model of three different approaches: neutral response, positive response and critical response (Allison 2002, p. 5ff). Following the neutral response approach innovation in the area of information technology is a phenomenon of contemporary development like telephones or washing machines have been before. Therefore, ICTs are becoming part of international politics but they do not influence or change them. The positive response approach says that ICTs have a high impact on political actors and therefore influence their behavior and decision making. The third approach (critical response) refers to the fact that access to ICTs is limited on a global scale and mainly occurs in industrialized countries and to a smaller amount in newly industrialized and developing countries. A lot of development studies are following this approach, dealing with the digital divide and other ICT4D topics.

The publications mentioned can be considered to belong to no specific Internet research area. They were mostly written within a certain research framework of classical international relations subjects (e.g. development or security studies). There is also no direct connection between publications like *The Internet Galaxy* (Castells 2001), *Open Networks, Closed Regimes* (Kalathil; Boas 2003) or *The Politics of Internet in Third World Development* (Hoffmann 2004).

However in the case of Internet governance it can clearly be spoken of an evolving research field. There is a growing but nevertheless still manageable number of monographies, anthologies and a selection of scientific articles and grey literature dealing with Internet regulation, ICANN, the IGF and different Internet policy fields. One reason for this is the ongoing process and debate about ICANN, WSIS and the IGF. Another one is the foundation of GigaNet which gave Internet governance research an institutional basis.

Milton Muellers *Ruling the Root* can be considered a central monography to understand the technical basics of the Internet and Internet governance. Mueller, Wolfgang Kleinwächter, Hans Klein and William Drake are some of the researchers who have been involved in Internet governance studies for several years. They (and others) have published on the Internet governance process and technical regulation from a global governance perspective. Some of the recent publications are *Internet Governance in a Global Multi-Stakeholder Environment* (Kleinwächter

2007), *The Internet and Global Governance: Principles and Norms for a New Regime* (Mueller; Mathiason; Klein 2007), *Internet Governance and the Information Society: Global Perspectives and European Dimensions* (Benedek; Bauer; Kettemann 2008), *Governing the Internet: The Emergence of an International Regime* (Franda 2001), *Multi-Stakeholder Governance and the Internet Governance Forum* (Malcolm 2008) and *Networks and States* (Mueller 2010). These general approaches towards Internet governance structures offer the basic principles to understand the framework and (historic) background behind Internet governance research. For this thesis they are an important part of the fundamental literature.

1.3 Objective

The objective of this thesis is to contribute to the relatively new interdisciplinary research area of Internet governance from an International Relations perspective. The author wants to analyze the opportunities and limits of a multi-stakeholder governance process. There is going to be a focus on the two sub-fields of Internet filtering and cybercrime to find out how the different stakeholders and actors participate and collaborate in these areas and how this affects the Internet governance process as a whole.

The Internet governance process is based on a multi-stakeholder approach how it was underlined both in the 2005-report of the Working Group on Internet Governance (WGIG) and the Tunis Agenda that was developed during the World Summit on the Information Society. Comparing Internet governance to other processes of global governance it becomes obvious that multi-stakeholderism is not dominating the field of global governance research. In fact there are few examples of multi-stakeholder processes while in the majority of cases governments are the only stakeholder parties (even though they sometimes include selected participants from other stakeholder groups). Actors in a multi-stakeholder environment like the IGF come from the public sector, private sector and civil society. Here it becomes clear how this approach can also be distinguished from private governance where civil society and private companies are both considered to be part of the private sector (Pattberg 2004, p. 12f). In multi-stakeholder governance processes not only the number of actors rises but there is also a higher diversity of interests in the

subject of governance. In the case of Internet filtering this becomes especially clear when looking at human rights organizations on the one hand and economic interests of IT companies on the other hand. Furthermore governments in countries that filter the Internet (e.g. China) consider it to be their sovereign right of content control.

While the problem of filtering shows the diversity of standpoints by different stakeholders that hardly seem to combine with each other, cybercrime demonstrates another challenge. There are different means of cybercrime like hacking, phishing, denial-of-service attacks, spam, and others. Some of them have an economical background, others have a political one. In many cases cybercrime is committed over national borders which not just makes it difficult to find out who actually committed the crime but also confronts national police forces with the problem that their sovereignty is limited to national borders. Furthermore due to the differences of various legal systems, acts committed in one country where they are considered to be legal can be a crime in another country. One example is the conflict between freedom of speech in the USA and racial discrimination in different European countries. In other cases the lack of a proper legislation regarding online activities can help certain people committing crimes in other countries by Internet. Cybercrime can even result in tensions between states like it was the case between China and Germany, the USA and the UK (Sueddeutsche.de 2007b; Spiegel Online 2007a; Spiegel Online 2007b). China was blamed for cyber attacks on different public institutions by the other three in 2007. While in these cases the attackers seemed to act from within Chinese government institutions the tensions between Russia and Estonia because of a cyber attack in the same year were obviously caused by private citizens (Kirk 2008). Already in 2001 the European Union presented a convention on cybercrime. But until today its effects are a subject of controversial discussion.

1.4 Relevance

In 2002 Mazarr explained in *Information Technology and World Politics*:

> This volume examines a subject that has so far received scant attention, at least in terms of formal, rigorous research projects: the effect of information technology on world politics, and specifically the growing role of the

> Internet in promoting freedom and changing social and political norms. (Mazarr 2002, p. 1).

While until 2010 the number of research projects concerning politics and the Internet has risen, one could repeat this phrase about the lack of attention regarding Internet governance studies and especially with an international relations approach. As mentioned before, there has been a small (but growing) number of academic research projects and publications since WGIG has developed the first definition of Internet governance in 2005. However, few of these projects use a political science approach and almost none comes from the area of international relations. Although the theoretical framework of international relations offers a variety of opportunities to include this topic into its area of studies. This refers not just to the global governance approach used in this thesis but also to the analysis of international conflicts, international organizations, development studies or regime construction just to name a few.

The Internet is not a temporary phenomenon but a technology that is going to stay and that is already dominating a big part of life of citizens, companies and governments. Cybercrime and Internet filtering are also of increasing significance. The non-territorial character of the Internet does not favor national solutions and for this reason the Internet governance process is happening on an international level. However, there are also governments that speak out for solutions on the national level. The conflict between these two basic models has just begun which underlines the relevance of analyzing details of this debate from an international relations perspective.

1.5 Research Questions

The central research question is:

How does the multi-stakeholder environment of the Internet governance process affect the phenomenons of cybercrime and Internet filtering?

There is a number of sub-questions that have to be considered as well:

a) How did multi-stakeholder governance processes develop in the past?

b) What stakeholders are involved in the Internet governance process?

c) What are the interests of different stakeholder groups concerning cybercrime and Internet filtering?

d) How do stakeholders act in the fields of cybercrime and Internet filtering?

e) How do different stakeholders cooperate or blockade each other?

f) How does cooperation or non-cooperation between different stakeholder groups affect the governance process of cybercrime and Internet filtering?

g) What conclusions can be taken concerning the multi-stakeholder governance approach based on the analysis of the two fields of cybercrime and Internet filtering?

Hypotheses:

a) The character of open discussion provided by the Internet Governance Forum will lead to a productive exchange of ideas used by all stakeholder groups. Nevertheless there will hardly be any global binding contract or convention between all stakeholder groups due to the diverging and hardly combinable interests. Instead there will be a number of partly agreements between different stakeholders.

b) Although all stakeholder groups have different interest, differences between the private sector and the governmental side (especially in the case of Internet filtering) will be settled much more easily than between civil society actors and the other two stakeholder groups.

c) In the case of cybercrime stakeholders will agree more easily on conventions than in the case of Internet filtering as the first is considered to be a virtual threat to all stakeholders while the other one is seen as a question of sovereignty and financial interests versus human and democratic rights.

d) There is a possible relation between cybercrime and Internet filtering. An increase of cybercrime

activities can lead to a higher degree of Internet filtering. An effective international protection against cybercrime can lead to a reduction of Internet filtering.

e) Without international conventions cybercrime will result in a limitation of basic rights (and human rights) in authoritarian as well as in democratic states.

1.6 Research Methods

This thesis is developed using a qualitative case study research design. “A case study (...) is the analysis of an object: a country, a political system, an institution, an organization, or a problem in a certain context (...). In a comparative analyses different cases on the same topic are used.” (Nohlen 1994, p. 128, *translation by the author*). A case study is one of the most applied methods in political research. Its origin goes back to 1948 at Harvard University (McNabb 2004, p. 357). It helps to explain an individual case and is also able to make a generalization (although quantitative methods are stronger for generalizations). It can be conducted with one or several cases. “Through the study of cases, political scientists are able to learn about political events, agencies, parties and levels of government and politics around the globe. Cases are also written to serve as examples of approved management practices.” (idem).

Robert Stake (1994, p. 237) divides case studies into three categories: intrinsic, instrumental and collective case studies. This way he tries to differentiate the motives of the researchers. An intrinsic study aims at understanding the case itself. The case is the central aspect of the study. The objective is nor the development of theories neither the analysis of a phenomenon behind the case. An instrumental study treats the case as an example for a theory or a political or social phenomenon. This phenomenon is the actual interest of the researcher. The case helps to explain it. The third category is a collective case study. The researcher uses it to investigate several cases that help to explain a certain phenomenon. Similar to Stake, Robert Yin divides case studies into two categories: single-case studies and multiple-case studies (Yin 2003, p. 39ff). Both have the intent to explain the phenomenon behind the case. John Gerring includes units of analysis in his definition of a case study. Therefore he defines a case study as “an intensive study of a single unit for the

purpose of understanding a larger class of (similar) units" (Gerring 2004, p. 342).

This thesis is analyzing the multi-stakeholder environment of the Internet governance process with a special focus on the two cases of cybercrime and Internet filtering. It is a multiple-case study (n=2) that will help to a) analyze the phenomenons of cybercrime and Internet filtering, b) analyze different stakeholder groups involved in the Internet governance process and their relations to each other, c) make general statements about Internet governance and multi-stakeholder governance processes.

The following four types of sources of evidence have been used:

1) **document analysis:** scientific literature, newspaper articles, documents and grey literature published by different stakeholder groups and during institutionalized meetings like the WSIS, IGF and others.

2) **direct observation:** observing stakeholder meetings at the Internet Governance Forum and online (some public meetings of stakeholders or institutions like ICANN are transmitted online on the Internet).

3) **unstructured interviews:** interviews and conversations with participants of the Internet Governance Forum and other individuals involved in the Internet governance process.

4) **structured interviews:** detailed questionnaires developed to get specific information from researchers and experts involved in the Internet governance process.

1.7 Structure

The thesis is structured into this introduction (chapter one), four thematic parts (chapters two to five) and a conclusion (chapter six).

The second chapter concentrates on the two phenomenons of global governance and multi-stakeholder governance. In there, an analysis of the current state of the art concerning the two theoretical concepts is conducted. Multi-stakeholder governance will be put into a historical and conceptual context. Furthermore will be discussed how and why multi-stakeholder environments have developed in the past years.

The third chapter concentrates on the Internet governance process. It includes a historical introduction regarding the origins and the development of the Internet. In this context also its technical functionality will be mentioned which is important especially to understand the details of the following case studies. Besides that, the main actors are discussed in this chapter, among them IANA and ICANN, as well as the UN process including WSIS, WGIG and the IGF.

The fourth chapter includes the first case study focusing on cybercrime. Therein, cybercrime is explained within the wider framework of cybersecurity including other forms of security issues like cyberwar or cyber attacks in general. It is important to understand the relation between the different categories as most cyber attacks are related to different forms of cybercrime, no matter if there is a political or an economical background. The relations between ordinary cybercrime and politically motivated cyber attacks become apparent by analyzing examples of cyber conflicts involving Russia, Estonia, Georgia and also China. Besides that, there will be a focus on international and regional organizations as well as civil society.

Chapter five is the second case study and deals with the problem of Internet filtering. To understand this phenomenon it is necessary to remind the technical functionality of the Internet given in chapter three. And it is also necessary to understand the technical methods used to manipulate the free flow of information online. For this reason the central methods of Internet filtering will be discussed. Furthermore, a number of didactical models will be included into the chapter to explain the reasons and ways governments are filtering the Internet. The idea of these

models is to support the argumentation of the case study but they can also be applied in other contexts. For example in international relations classes which are dealing with Internet filtering as an issue of international politics. After that, filtering processes in non-democratic and in democratic countries will be discussed. Emphasis will be given on the Chinese filtering system (which is among the most sophisticated at the time) and on the European debate on Internet filters, especially in Germany.

In the last chapter the results of the study will be taken up to develop final conclusions on the individual topics of the thesis and on the research project as a whole.

Chapter Two: Global Governance

The fall of the Berlin Wall on 9 November 1989 marked not only the end of the bloc confrontation that dominated international politics far beyond Europe for more than four decades, it also ended a period in which national sovereignty was considered the only determinant concept and national governments the only decisive actors in international affairs. The changing political and economic relations between old and new states, the growing influence of civil society as a global actor, new locations, challenges and forms of violent conflicts, growing awareness of ecological issues and climate change, the increasing use of new information and communication technologies and more paved the way for new forms of alliances, new alignments of actors and interest groups, new agendas and forms of discussion. For about half a century inter-state conflicts had been dominating the agenda of international politics making realism the main theoretical concept of analysis in international relations. During the Cold War little space was offered for international cooperation. However, with an accelerating process of economic interactions since the late 1970s Keohane and Nye analyzed the increasing interdependence between a variety of actors on the global stage. This interdependence was defined as "mutual dependence … in world politics [which] refers to situations characterized by reciprocal effects among countries or among actors in different countries" (Keohane; Nye 2010, p. 7). The interdependence theory is one of the basic concepts of the global governance approach. A second one is the concept of globalization.

Globalization belongs to the most mentioned, analyzed and ripped apart post-1989 concepts. Different than interdependence or global governance it became popular also outside the scientific community and made its way into non-academic debates and daily newspapers. Following Woods globalization can be defined as a "combination of internationalisation, political and economic liberalisation, and a technological revolution" (Woods 2002, p. 25). Others like Sklair challenge the expression of "internationalisation" stating that one of the core aspect of globalization is the plurality of actors besides states while *inter*-nationalisation would refer mainly to nations or nation-states (Sklair 1999, p. 234). In fact, processes of globalization also include amongst others civil society actors, private companies and international organizations.

Although the concept of globalization spread in academic debates only after the end of the Cold War the phenomenon itself is not limited to this short period of history. Economic and cultural

expansion and interaction have taken place in many moments of history. George Modelski set the initial point of globalization at about 1000 years ago when a large part of the world from Eastern Asia to Western Europe was under the rule of an Arab empire (Modelski 2003, p. 55). However, constant changes since then and the end of the 20th century make clear that other concepts than globalization should be applied to analyze the centuries in between.

While in the past 20 years the term globalization had been used in many imaginable contexts it became an almost empty expression over the years. In academic discussions today globalization often goes hand in hand with global governance which instead of trying to describe and analyze the phenomenon of globalization itself is concentrated more on the question of how to rule new global constellations which resulted from it. Constellations that after the end of the Cold War changed governance on a world wide scale (Rosenau; Czempiel 1992, p. 1). Changes that following Rosenau "are surely profound and extensive, and their consequences are surely bound to be enormous for decades to come..." (idem, p. 23).

Similar to Modelski's approach regarding historical roots of globalization, also the concept of global governance shows a temporal divergence between the upcoming academic debate and the historical origins. While the post-Cold-War era marks the period of time in which global governance became a paradigm of analysis, Murphy identified its first appearance to have happened long before:

> The historically minded like to remind us that something like "global" governance has been emerging ever since the European conquests of the fifteenth century. By 1900 the world was pretty much divided into colonies and zones of interest of the European powers, the United States, and Japan, and a weak system of inter-imperial institutions – the gold standard, the balance of power, European international law, and the first global international organizations – regulated the whole. (Murphy 2000, p. 790)

Nuscheler (2002, p. 78) suggested that first elements of global governance can be found already in Kant's idea of a federation of republics and therefore in the concept of perpetual peace which was published in 1795.

In 1992, only three years after the symbolic end of the East-West conflict, Rosenau concluded that the global agenda and its actors had already changed extensively. Together with

Czempiel, Rosenau presented the volume *Governance Without Government*, which is considered a pathbreaking work for the debate on global governance, although, as Hewson and Sinclair (1999) observed, the term itself does hardly appear in any of the contributions to the book. Rosenau and Czempiel identified some of the leading questions which were going to influence the debate for the coming years, including 1) how to operate governance processes on a global scale without having a global government and 2) who would be responsible for developing and implementing global rules if there was no global government (Rosenau; Czempiel 1992, p. 1). Rosenau also referred to the new multiplicity of actors that had already entered the global stage and were about to reduce power of governments as the former traditionally dominating actors in international politics:

> During the present period of rapid and extensive global change (...) the constitutions of national governments and their treaties have been undermined by the demands and greater coherence of ethnic and other subgroups, the globalization of economies, the advent of broad social movements, the shrinking of political distances by microelectronic technologies, and the mushrooming of global interdependencies fostered by currency crises, environmental pollution, terrorism, the drug trade, AIDS, and a host of other transnational issues that are crowding the global agenda. (…) Governments still operate and they are still sovereign in a number of ways; but (…) some of their authority has been relocated toward subnational collectives. (idem, p. 3).

Dingwerth and Pattberg (2006) use three different categories to distinguish the concept of global governance: 1) global governance as an analytical concept to understand the reality of contemporary world politics, 2) global governance as a specific political program to react on the loss of governmental power during the process of economic globalization, and 3) global governance as a specific academic and social discourse from a critical perspective (Dingwerth; Pattberg 2006, p. 378). These three categories will serve as a framework to discuss the concept of global governance in the following paragraphs.

Within their first category Dingwerth and Pattberg refer to Rosenau's definition of global governance: “global governance is conceived to include systems of rule at all levels of human activitiy – from the family to the international organization – in which the pursuit of goals through the exercise of control has transnational repercussions“ (Rosenau 1995, p. 13). What Rosenau describes as “all levels of human activity“, is the variety of new actors that play a central part in global governance. Although they are not new in respect to their existence, they are new when it

comes to their role in international politics. While in previous decades before 1989 national governments were seen as the central and only crucial actor in international politics, global governance includes a multitude of actors many of them from civil society and the private sector which now operate with a growing independence from national governments. This development goes along with a gradual reduction of hierarchies between different groups of actors as well as between different forms of governance. In this context a multilayer governance system is established in which local, national, regional and global processes are inseparably combined, and where new spheres of authority are operating independently from nation states (Dingwerth; Pattberg 2006, p. 381ff). Karns and Mingst (2004) mention the following organizations and individuals as being the principal actors in global governance: states, intergovernmental organizations (IGOs), non-governmental organizations (NGOs), experts, global policy networks, and multinational corporations. Intergovernmental organizations are sub-types of international organizations (IO). Another IO sub-type would be international non-governmental organizations (INGOs). Regarding NGOs the authors distinguish in a larger number of sub-units which are used to refer to a specific function of each organization (Table 1).

Table 1

NGO Sub Units	
AGO	antigovernmental organization
TRANGO	transnational NGO
GONGO	government-organized NGO
GRINGO	government-regulated and initiated NGO
BINGO	business and industry NGO[15]
DONGO	donor-organized NGO
DODONGO	donor-dominated NGO
ODANGO	ODA-financed NGO (ODA = official development assistance)
FLAMINGO	flashy-minded NGO (representing rich countries)
PO	people's organization
ONGO	operational NGO
ANGO	advocacy NGO
TSMO	transnational social movement
GSM	global social movement

Source: Karns; Mingst 2004, p. 18

[15] BINGO can also refer to Business International Non-Governmental Organization, a private sector sub-type of an international organization (Woyke 1995, p. 189).

Besides that, they introduce another unit of analysis called *pieces of global governance* which are defined as “cooperative problem-solving arrangements and activities that states and other actors have put into place to deal with various issues and problems“ (idem, p. 4). These include 1) international law, 2) international norms or soft law, 3) formal and informal structures (NGOs, IGOs, G8 etc.) and 4) international regimes. In this regard the main actors of global governance mentioned above fit into the third group of pieces of global governance.

In Dingwerth's and Pattberg's second approach they refer to the question how societies do or should react to new global constellations. An often mentioned example for this normative approach to global governance is the report of the Commission on Global Governance (Our Global Neighborhood) which was completed in November 1994 and published in 1995. The Commission on Global Governance (CGG) was “an independent group of prominent international figures, formed to consider what reforms in modes of international cooperation were called for by global changes“ (Karns; Mingst 2004, p. 3). Some of its members were Enrique Iglesias (President of the Inter American Development Bank), Hongkoo Lee (Prime Minister of the Republic of Korea), Yuli Vorontsov (Russian Ambassador to the United States), Barber Conable (former President of the World Bank), and Allan Boesak (former South African Minister for Economic Affairs). The CGG defined governance as a concept (and global governance in particular) as:

> the sum of the many ways individuals and institutions, public and private, manage their common affairs. It is a continuing process through which conflicting or diverse interests may be accomodated and co-operative action may be taken. It includes formal institutions and regimes empowered to enforce compliance, as well as informal arrangements that people and institutions either have agreed to or perceive to be in their interest. (…) At the global level, governance has been viewed primarily as intergovernmental relationships, but it must now be understood as also involving non-governmental organizations (NGOs), citizens' movements, multinational corporations, and the global capital market. Interacting with these are global mass media of dramatically enlarged influence. (CGG 1995, p. 2f).

Similar to Rosenau's different “levels of human activity“ the CGG report also underlined the importance of new actors in global governance. The importance of the variety of actors is shown in the report, where topics as diverse as military transformation, social and environmental change, demilitarization, international trade, migration and global civil society are discussed. Comparing present-day situations (2010) with statements made in the CGG report fifteen years before it

becomes clear that especially in the first decade of the 21st century the interaction between actors in different policy fields has evolved more than it was imaginable at the time the CGG was constituted. One example is the convergence of development and security, two policy fields that were following very diverging interest during the Cold War. Although development policies and aid financing were closely connected to Western foreign policy interests during the Cold War, a lot of civil society actors in that field had their roots in a number of different political movements like humanitarian groups, religious groups, pacifist groups and the peace movement. Until the break-up of the Soviet Union there were hardly any commonalities between them and Western military. In fact, civil society's associations with military operations were rather related to violence and destruction than humanitarian support. One of the main reasons for this was the 20-years-lasting Vietnam war. Another one was the fact that developmental actors were often working in areas where violent conflicts and war had caused severe destruction. On the other hand humanitarian activists and NGOs were considered opponents or at least obstacles by the military. After 1989 this paradigm changed for a number of reasons.

In January 2001 the UN Security Council discussed the problem of HIV in a number of African countries, which was far from being a traditional security topic (UN 2000). In the following years a number of issues regarding health, environmental and social policies were included into the global security agenda. Also the concept of human security became part of these changes. It was established on the argument that security was not anymore based on the defense of a state or the defeat of its adversary but on an accumulation of problems related to the individual human being. As King and Murray (2001, p. 588) put it: “These debates led to calls to consider security from a global perspective rather than only from the perspective of individual nations and the idea of common security.“ Against this background, security forces and development agencies became partners in several areas, among them post-conflict nation building or the restoring of statehood (Klingebiel; Roehder 2004). Another example of the changing constellations is the approximation of civil society and the private sector, especially large companies. While in the past these actors were considered opponents they partly closed ranks in the post-Cold War era. This can be seen for example on the basis of cooperation between human rights groups and pharmaceutical multinationals (Amis; Leisinger; Schmitt 2004).

The third approach developed by Dingwerth and Pattberg refers to authors like Ulrich Brand and Henk Overbeek who take critical standpoints on the global governance discourse. Their focus lies on the question if the global governance discourse merely serves to cover the negative implications of neoliberal ideology and practice. And furthermore they criticize the covering of existing conflicts by a debate that creates an image of cooperation. The authors themselves declare that global governance can be seen as a twin phenomenon of globalization rather than a force to control it (Dingwerth; Pattberg 2006, p. 386f). Regarding the diversification of actors they explain that although a variety of them is included in global governance processes, the structural relations of power and hierarchical configurations of social reality are being ignored (idem).

In 2006, 14 years after Rosenau's basic work on global governance, Messner and Nuscheler pointed out that they still saw global governance research in its initial phase. They described current debates as a phase of orientation, comparable with the early years of the debate on sustainable development (Messner; Nuscheler 2006, p. 44). The authors identified six crucial aspects that need to be considered to bring forward and to consolidate global governance research (idem, p. 44ff).

The first aspect concentrates on the question of transferring issues from the local to the global level. So far, global governance research is taking its theoretical framework from a number of approaches, being especially international relations theories, but also theories applied to analyze local, national or regional aspects. Besides that, the authors suggest considering approaches used to analyze European constellations (both authors are from Germany) as well as social science steering theories (idem, p. 45). Although the inclusion of different frameworks can be helpful for the formation of global governance theory it is important to remember that an adaption to the new scenario is necessary. Transformation theories based on empirical evidence in for example the European Union, will not serve to the same degree in a global scenario. They need to be adapted especially concerning the higher quantity and the qualitative diversity of the actors involved. Another important point mentioned by the authors is the cultural diversity on a global level which automatically includes different ways of perceiving and resolving problems (idem). At the same time cultural beliefs, ethnicity and other forms of collective values can counteract processes of global governance and lead to a separation rather than a consolidation of different actors, if insufficiently applied transformation processes are turning citizens away from the global and towards a local scenery.

The second aspect is the necessity of empirical research. Since global governance was defined as a new research area, studies were conducted mainly on the problem of structural changes in international politics. In this context a focus was given on theoretical approaches while less empirical research has been done. Since Messner and Nuscheler articulated this criticism things have changed and especially in the first decade of the 21st century the number of empirical research projects with a global governance background has increased. However, there is still need for more as aspect three indicates.

The exigency for further empirical research on actors, regimes and other “pieces of global governance“ (Karns; Mingst 2004) becomes clear when considering global governance a composition of a multitude of aspects deriving from a diversity of actors, regions, countries and other “pieces“. In their third point Messner and Nuscheler (2006, p. 50) refer to global governance as a macro perspective which is built on countless empirical research results. A high quantity of empirical research will therefore contribute to an improving understanding of global governance as a phenomenon itself. This conclusion actually is not confined to this specific area of study but can be seen as a general statement in favor of the case study design. As mentioned in the first chapter, case studies serve to find evidence on social phenomenons by analyzing their details. This study can therefore be seen as an intention of analyzing “pieces“ to contribute to the macro perspective of an underlying global phenomenon.

The fourth aspect refers to the existence of two schools of thought within the global governance approach and their dissociation. On the one hand the authors located followers of a traditional approach concentrating on classical subjects as power, hegemony or geopolitics in a nation state context, focusing mostly on security and natural resources (idem, p. 51). On the other hand there are those analyzing global problems and their solutions, especially focusing on new topics of the international agenda. Without immediately naming it, it becomes clear that the authors are referring to the representatives of two of the principal theoretical approaches in international relations, being realism and liberalism/institutionalism. To develop an all-embracing concept of global governance they suggest an approximation of the two schools of thought to compare their theoretical frameworks and to develop new concepts beyond traditional approaches.

The next aspect addresses the question of interdisciplinarity. Although the debates on global governance are taking place mostly in the areas of political science and international relations there is a number of additional fields that are touched as well. As mentioned before, worldwide changes termed globalization (which are closely connected to global governance) have a strong focus on economic transformations. In classical political science and international relations thinking, a deeper understanding of economy has a more or less marginal position (disregarding political economy). To understand economic globalization it is necessary to have a comprehensive knowledge of specific issues, e.g. the structures of financial markets. On the other hand pure economists usually have less understanding of political systems or social effects of transformation processes. At this point the importance of an interdisciplinary approach becomes obvious. But not only political and economic science should enter into a symbiosis to improve their outputs. The large scope of problems related to global governance requires cooperation between a number of areas in which political science or international relations researchers are involved. The already established focus of global environmental studies for example premises also the exchange with natural scientists (idem, p. 53). As the topic of this thesis suggests, political scientists furthermore need to connect to computer, informatics or telecommunication researchers to get a better understanding of the technical side of Internet governance. In fact, Internet governance is already an interdisciplinary area. But it has few members of the political science community and even less members of the international relations community. In this thesis it will become clear that this will be a challenge in the coming years, especially as decision makers in the public sector often use their standard policy procedures without holding the necessary knowledge about the subject matter. This can not only lead to ineffective policies but may also harm decision makers' reputation as competent representatives.

The sixth and last aspect of Messner's and Nuscheler's discussion of the status quo of global governance research in the early 21st century concentrates on the separation of different levels of analysis in a multi-level governance system (idem, p. 54). These levels are defined as local, national and international layers which are individually investigated by different scientists. The main criticism of the authors is directed to the fact that the majority of scientist treat these levels separately as if they were not connected to each other, which is not the case. Instead of treating global governance as such a system of separately analyzed layers, the authors recommend to take into account the interaction of the different levels.

While the before mentioned authors (especially Keohane, Nye, Rosenau, Mingst and Karns) had specified the new diversification of actors on the global stage, the German sociologist Ulrich Beck is investigating the reasons for their strengthening. In his analysis of a “risk society“, in which he refers mainly to civil society groups and individual parts of the population, he presents fear as a crucial factor of mobilization (Beck 1986). According to this, progress, modernization and also globalization are creating a growing number of risks which can be manifested in globally spreading diseases, natural and environmental disasters or result in simple uncertainness about how technological innovations will influence life. The increasing quantity and quality of risks is overburdening public institutions which opens spaces for other actors. This political vacuum is then filled by civil society groups. These organizations and initiatives are formed by citizens who, driven by fear, decided to become active members of their respective societies (idem, p. 62). The strengthening of civil society and the growing political participation outside the traditional governmental structures have a weakening effect on the political system (idem, p. 311). This way a circuit of decreasing traditional power and an increasing participation of other actors is forming. In this context the political vacuum caused by growing political participation of citizens can also be filled by the private sector.

Beck's first concept of a risk society was developed in the 1980s in a Western-European context and needs to be understood under the structural, regional and economical circumstances of that time. The profound changes in international politics in the post-Cold War era led to an extension of his approach. In 2007 he published his analysis of the world risk society, taking his earlier concepts on a global level (Beck 2007). While before, the actors of his theories were mostly of local or national character they are now appearing on the global stage. Transnational civil society organizations are for example controlling or cooperating with multinational companies and global risks still play an important role in democratization processes (idem, p. 117). And still fear is the driving factor of political participation and as a consequence of global democratization.

Analyzing Beck's approach under Messner's and Nuscheler's criticism towards global governance research one thing becomes clear. It is the necessity to verify if Beck's theories can be easily applied on a global scale or if they need to be tested and adapted before. Beck's argumentation that changes are causing fear and lead to political participation and democratization has a strong focus on the German society. Although Germany has an international reputation for

being a country of technological innovation there is also a strong tendency within the population to object new technologies and social changes. This phenomenon is also known as “German Angst“ and is sometimes characterized by a certain disposition to hysteria and exaggeration of risks (Güntner 2011). One example is the rejection of the *Transrapid* high speed train technology which was developed in Germany over decades but since 2004 is only used in China. An installation in Germany failed due to public denial. Another example are the strong protests against Google Street View, an Internet photo service that saw itself confronted with (even violent) objection by a large part of the German population, including members of the government (Fischer; Medick; Peters 2010). Mistrust caused by progress can be seen as a common characteristic of the German society. Beck's analysis is therefore helpful to understand the relations between globalization, participation and global governance in Germany and maybe other European states. However, it cannot be transfered to societies in South America or Asia for example, which have a very different perception of risks and the appropriateness of reactions to them.

Nevertheless, Beck joined the group of authors dedicated to the emergence of new actors, also known as new stakeholders in the multi-stakeholder environment. The multi-stakeholder governance model which is a central component of this thesis is both part of the global governance idea and its consequent continuation. As mentioned above, the appearance of new actors besides states is a crucial aspect of global governance. However, it needs to be distinguished between governance constellations which are dominated by governments and those in which other actors are included as well. Beyond that, in constellations consisting of different actors it needs to be considered which hierarchical positions they are taking. Dingwerth's and Pattberg's observations regarding the gradual reduction of hierarchies between the multitude of new actors, play an important role in the next chapter which will concentrate on the development of the multi-stakeholder approach in international cooperation. This form of global governance represents the lowest hierarchical barriers between all relevant stakeholder groups.

2.1 Multi-Stakeholder Governance

Right from the beginning the Internet governance process was constituted as a multi-stakeholder process. Just like Internet governance also multi-stakeholderism is a relatively new form of governance that has not been extensively investigated. Levinson and Smith call it an "understudied phenomenon" (2008, p. 16). It is the result of global changes in cooperation and diplomacy that took place in recent years and can be traced back to the beginning of the 1990s when due to the end of the East-West conflict old alliances underwent profound changes. At the same time the importance of the private sector and civil society became clearer. This development had already started during the Cold War but due to international constellations it continued at a much slower speed. What happened at a limited extend during the Cold War accelerated in the 1990s and later resulted in the multi-stakeholder governance approach which will be discussed in this chapter.

To comprehend how governance changed in recent years it is important to take a look at its different stages in the history of the United Nations (UN). Jens Martens (2007, p. 11) offers a three-phases-model to understand the basic changes that were happening since the 1940s (especially after 1945) and which lead to the inclusion of several non-state actors in international negotiations. The model is separated into three time segments: 1) 1940s – 1960s, 2) 1970s – 1980s, and 3) after 1989.

The beginning of the first phase was dominated by the reconstruction after the Second World War and the beginning of the Cold War. This dawning era of bloc confrontation and proxy wars saw the domination of the realist perspective in international relations. Politics at that time happened mostly among governments (Clinton; Morgenthau; Thompson 2005). This was also the case during the era of decolonization in the 1960s when states still dominated the scenario, leaving little space for non-state actors. Although already at that time a few NGOs participated in different UN processes, and also actors from the private sector like the International Chamber of Commerce, which was categorized as an NGO as well (Martens 2007, p. 12). Nevertheless their influence was marginal, compared to the changes in the following decades.

During the second phase (1970s-1980s) confrontation between states was still dominant. Anyhow non-state actors were winning more ground. This had already started partly in the second half of the 1960s and went on until the end of the 1980s. Crucial occurrences happened in both the

occidental and the oriental parts of the world. In capitalist countries (and their allies) the U.S. civil rights movement, the student protests in France, Germany, Brazil, Mexico and others, as well as the mobilization against the Vietnam war were initial events. Later a growing number of NGOs and social movements came up, many of them in support of social development in countries that recently had achieved their independence in what was (and sometimes still is) called the Third World. In this wave of new upcoming civil society groups several new topics were set on the agenda that did not get the attention of national governments (Halliday 2001, p. 24f). Among them were environmental questions, womens' rights, and disarmament. Originating from protest movements, many NGOs did not seek for cooperation with national governments and also governments themselves showed little interest to give support to those new and to a certain grade still unprofessionally working organizations[16]. This position was maintained also within the UN system for which reason civil society groups agitated mainly in opposition to the political establishment. Besides new NGOs and social movements, also private sector companies started getting more influence in political processes. Especially multinational enterprises were eager to improve their already existing relations with national governments. At the same time they remained mostly skeptical towards the UN by whom they saw themselves criticized for working conditions and uncontrolled international business activities (Martens 2007, p. 12).

Also communist countries saw the appearance of social movements like for example in Hungary, Czech Republic, Yugoslavia and Poland. Although their development was different compared to movements in Western countries, some of them became very influential during the transition processes after 1989 (Linz; Stepan 1996, p. 230ff).

The third phase was marked by the fall of the Berlin Wall, the collapse of the Soviet Union, and as a result the end of the bloc confrontation. At that time, the role of national governments was not only to be redefined, there was furthermore a certain decrease in governmental influence which was also related to a growing neoliberal ideology reducing state intervention in several areas (Martens 2007, p. 11). This political vacuum was a welcome opportunity for non-state actors to expand their own sphere of influence (a phenomenon that Beck had already analyzed in the 1980s). Deregulation, privatization, and the growing importance of global topics like environmental issues, climate change, migration, poverty reduction, health care and others prepared the ground for an

[16] For more details on relations between NGOs and states see: Ahmed; Potter 2006, p. 57ff.

environment in which public, private and civil society actors (stakeholders) approached each other to solve old and new problems of the post-Cold War era. Some of these topics that now appeared on the international agenda had already played an underpart in the decades before. Climate change, indigenous and minority rights or children's rights that had mostly been ignored by governments before, were now areas where civil society organizations had developed special knowledge over the years and due to their long-time dedication also legitimacy by the social groups they were working with. This made them important partners for national governments who did not have a lot of experience in those fields. The power shift from the public sector to non-state actors can be reconstructed with the help of Hocking's example of trade policy (Hocking 2006, p. 21ff). With the growing number of global tasks, the question of financing had to be resolved as well which was where the private sector had to come in. In exchange, private companies gained support from the public sector to improve their investment strategies in different countries. By cooperating with civil society actors they also managed to improve their image as socially responsible companies. This became an important question in their marketing strategies.

Two key events that included civil society and the private sector into the global governance scenario happened in the beginning and at the end of the 1990s. That decade was marked by a number of global conferences underlining the new international political agenda (Fues; Hamm, 2001, p. 50). In 1992 the UN Conference on Environment and Development took place in Rio de Janeiro. It was therefore also known as the Rio Summit or the Earth Summit. During that conference a variety of topics was discussed that had a special importance for civil society actors. These topic were related to rural development, women's and children's rights, climate protection and several environmental issues. One of the results of the conference was the Agenda 21, a strategic document focusing on global sustainable development. The Rio Summit was a crucial moment for civil society as most (if not all) of the topics debated had been on the agenda of innumerous NGOs and other non-profit-organizations for a long time already. The Earth Summit was a decisive moment when they could carry their expertise onto the global stage to share it with government representatives and an international public. This way, the Rio Summit emphasized the importance of the integration of new stakeholders (in this case civil society actors) into international governance processes. It was therefore a key event for the development of the multi-stakeholder approach.

The second inclusive event was the Global Compact which UN Secretary-General Kofi Annan presented in 1999 at the World Economic Forum in Davos. The idea of this voluntary framework was to bring the private sector together with those actors already involved in the new global agenda.

> The Secretary-General challenged individual corporations and representative business associations to demonstrate good global corporate citizenship by embracing nine [later ten – the author] principles in the areas of environment, labour and human rights, and by advocating for stronger United Nations organizations in those and related areas. (Kell; Ruggie 1999, p. 101).

By including the private sector into the scenario of global governance the UN and indirectly also civil society became access to fundings that were necessary to accomplish the challenges and new programs developed throughout the decade of the 1990s. However, not only the financial question but also the political message was clear: private companies participating in the agreement declared to respect the principles set up by the UN referring to the policy fields mentioned above (environment, labor, human rights) plus a commitment regarding anti-corruption practices (Table 2). The principles were based on the Universal Declaration of Human Rights, the International Labor Organization's Declaration on Fundamental Principles and Rights at Work, the Rio Declaration on Environment and Development and the United Nations Convention Against Corruption. Also the private sector realized the advantages of cooperation. By respecting the principles of the Global Compact it was receiving support by the UN, supporting the creation of business-friendly environments which resulted in the development of new, stable markets and investment areas. In 2008 a study conducted by researcher at the Technical University of Darmstadt (Germany) was indicating that companies participating in the Global Compact had made progress regarding corporate social responsibility. In a gradual model consisting of five levels, most companies had reached the third level in which corporate social responsibility measures were integrated into management processes. However, the researchers also criticized the lack of commitment in certain areas like human rights protection (Rieth 2008).

Table 2

Ten Principles of the UN Global Compact	
Principle 1	Businesses should support and respect the protection of internationally proclaimed human rights; and
Principle 2	make sure that they are not complicit in human rights abuses.
Principle 3	Businesses should uphold the freedom of association and the effective recognition of the right to collective bargaining;
Principle 4	the elimination of all forms of forced and compulsory labor;
Principle 5	the effective abolition of child labor; and
Principle 6	the elimination of discrimination in respect of employment and occupation.
Principle 7	Businesses should support a precautionary approach to environmental challenges;
Principle 8	undertake initiatives to promote greater environmental responsibility; and
Principle 9	encourage the development and diffusion of environmentally friendly technologies.
Principle 10	Businesses should work against corruption in all its forms, including extortion and bribery.

Source: UN Global Compact

The question that comes up now is what distinguishes global governance, a governance form that includes actors from all parts of society, from a multi-stakeholder governance approach. An important aspect to answer this question is not *who* is participating but *how* participation is happening. The democratization of international affairs resulted in a multiplication of actors (Ahlert 2001, p. 67f). Nevertheless, this tendency can be considered a decentralization of international politics but not an equalization of its actors. In traditional global governance processes and especially in international organizations, governments still have the main influence and are considered the central actors that cooperate with other organizations from business or civil society in particular moments. The private sector and civil society have strengthened their positions but are not completely included into official governance processes. That means they can be consulted by governments or cooperate among each other but have to stay outside when governments discuss and decide about crucial issues. A pivotal aspect of multi-stakeholder governance is therefore the inclusion of all actors into the entirety of a governance process. Haufler (2003) differentiates in her economy-based approach between four types of governance (which she calls regulations): 1)

traditional regulation (governments only), 2) co-regulation (governments and the private sector), 3) industry self-regulation (private sector only) and 4) multi-stakeholder regulation. Following her explanation, "multi-stakeholder regulation is differentiated from the other three types by the influential role played by non-profit groups." (idem, p. 239). Hocking (2006) categorized the multi-stakeholder approach as an emergent form of governance compared to the traditional state-centered approach (idem, p. 14). He also emphasized: "A fundamental premise of multi-stakeholder processes is inclusiveness and partnership in policy processes, rather than exclusiveness." (idem, p. 17).

Multi-stakeholderism became more influential especially in UN processes few years after the Global Compact was created. In 2002, the first truly UN multi-stakeholder conferences were hold in Monterrey (Conference on Financing Development) and Johannesburg (Summit on Sustainable Development). In both cases stakeholders from all areas of society were not just invited, but also (and this is the crucial point) involved in the preparatory phase. Furthermore, for the first time also individual companies instead of business associations could participate as actors from the private sector. Since then the multi-stakeholder approach has gained growing attention and was applied in several cases of international negotiations. This is also the case for the Internet governance process in which the multi-stakeholder approach became widely recognized as the leading form of participatory and inclusive governance. In this context a group of RAND researchers stated:

> Roles have often shifted among government, corporations and civil society (consider the Red Cross or the British East India Company's histories) but it appears that the United Nations is underwriting a more durable, multi-stakeholder relationship in regard to Internet governance. This is a novel and fascinating attempt to achieve real global dialogue around responsibilities in the Global Information Society, and may be a significant new governance paradigm. (Cave et al 2007, p. 5).

The multi-stakeholder governance approach can therefore be defined as a governance process based on the inclusiveness and participation of all actors from the public sector, the private sector, civil society and other relevant interest groups which meet on equal terms to discuss and decide together about a chosen topic.

Chapter Three: Internet Governance

The third chapter concentrates on the Internet governance process. In the beginning there will be a historical introduction to understand the development process of the Internet and to get to know some of the early actors involved. A lot of those actors, individuals and organization, have attended the Internet from the early days of basic network experiments until the 21st century. Some of them started as graduate students in computer research groups helping to set up the first networks and are now in leading positions of global Internet regulation organizations. Besides that, a closer look will be taken at the Internet Corporation for Assigned Names and Numbers (ICANN), the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF). All of the three are important "pieces of global governance" in the Internet governance process.

3.1 Historical Introduction

Talking about the historical aspects of the Internet seems to be unordinary as it is considered a relatively new technology. Today, the Internet is one of the most important or maybe even *the* most important means of global communication. It is not only transporting or offering access to information but is also a space of permanent innovation. These innovations happen in (at least) two distinct areas which are also visible for two different types of people: the developers and the users. Developers and programmers (or IT engineers) are in fact users as well while to majority of the users does not possess any knowledge of programming when it comes to languages like HTML, C++, php, delphi and others. Different than most users, programmers are realizing most of the innovations when it comes to written code which results in a lack of knowledge for those who are not frequently accompanying the latest developments. For this reason, books explaining programming languages are soon outdated after being published. But this is not just the case for literature on programming. Also political aspects, governance and regulation of the Internet are changing at fast speed in just a few years. One example is Lawrence Lessig's widely read book *Code*, which was first published in 1999 and then republished few years later in 2006 as a 2.0 edition starting with the sentence: "This is a translation of an old book – indeed, in Internet time, it is a translation of an ancient text." (Lessig 2006, p. ix).

However, the average user realizes innovation of programming and codes only indirectly through new functions he can use and which might change for example the appearance of a website he is visiting. In the early 90s, the optical appearance of the Internet was dominated by static HTML code. After a few years, the first dynamic websites came up, using animations and sound applications. Later also movies, instant communication and VoIP were integrated. The fact, that all these innovations happened in just a few years creates the illusion that the Internet does not have a longer lasting history. But in fact it has. This chapter is focused on the history of the Internet to understand the historical and political background of the network, as well as its basic functions. The sources used for this historical part were mainly written by those who observed or took part in this early process, among them Leonard Kleinrock, Vint Cerf, Jon Postel, Robert Kahn and J.C.R. Licklider.

On 4 October 1957 the Soviet Union launched the first artificial satellite in the world called Sputnik, which was shot into the atmosphere from Baikonur (today Kazakhstan). Sputnik had a diameter of 58 cm, a little bigger than a football. The successful launching was a surprise for the Western world and especially for the United States of America which suffered a shock comparing the technological progress of Moscow with their own. Until that day, the capitalist world had no doubt that is was in a technologically leading position. However, the plans of the Soviet Union were not kept secretly and also the Western World possessed official information about some of Moscow's scientific programs. The development of satellites had been discussed during the International Geophysical Year of the International Council of Scientific Unions which happened between 1 July 1957 and 31 December 1958 and which was supported by the United Nations. During these 18 months 67 states participated and presented their geophysical research projects. Moscow used this opportunity to present its plans for Sputnik and so also Washington was aware of the satellite. And also the U.S. had its own plans to enter into space with their satellite Vanguard. What in the end astonished the U.S. was the fact that Moscow realized a successful launch one month before Washington wanted to send out their own satellite. The competition between East and West was intense and this time Moscow had won the race.

As a reaction to Moscow's progress, Washington started funding a number of educational programs in the scientific and mathematical area. Furthermore, a number of research and development institutions was created. Through the National Defense Education Act a large number

of research scholarships was offered and schools were provided with scientific equipment. Another result of these reforms was the foundation of the Advanced Research Projects Agency (ARPA) within the Department of Defense (DOD directive 5105.15) by President Dwight D. Eisenhower on 7 February 1958 (Stine 2009).

3.1.1 ARPA

ARPA's responsibility was the development of space defense technology. In the same year of its foundation the part of ARPA responsible for space investigations and missile development was separated and moved to the National Aeronautics and Space Administration (NASA), leaving ARPA with the responsibility of computing research. ARPA, which did not have it own research laboratories, started financing a variety of research projects in different universities, among them the Massachusetts Institute of Technology (MIT). In October 1962 Joseph Carl Robnett Licklider (also known as Lick, 1915-1990), a mathematician and psychologist at MIT was appointed director of the Information Processing Techniques Office (IPTO) of ARPA, which was the department responsible for financing computation research. Before he became part of ARPA, Licklider had come up with the idea of a global network of computers to access information all over the world which he called the Galactic Network. In this context, Licklider had developed creative and progressive thoughts about the relation between human beings and computers. In 1960 he published the article *Man-Computer Symbiosis* discussing the advantages of the computer for human work. In an experiment Licklider discovered that within a good part of his own working hours he was using working techniques which could be performed with greater time efficiency by a computer and besides that would improve processes of thinking:

> The main suggestion (...) is that the operations that fill most of the time allegedly devoted to technical thinking are operations that can be performed more effectively by machines than by men. Severe problems are posed by the fact that these operations have to be performed upon diverse variables and in unforeseen and continually changing sequences. If those problems can be solved in such a way as to create a symbiotic relation between a man and a fast information-retrieval and data-processing machine, however, it seems evident that the cooperative interaction would greatly improve the thinking process. (Licklider, 1960, p. 5).

Besides that, Licklider came to the conclusion that verbal communication between human beings and computers would be an ambitious progress:

> (...) there is continuing interest in the idea of talking with computing machines. In large part, the interest stems from realization that one can hardly take a military commander or a corporation president away from his work to teach him to type. If computing machines are ever to be used directly by top-level decision makers, it may be worthwhile to provide communication via the most natural means, even at considerable cost. (idem, p. 13)

Today, 50 years later, keyboard and mouse are still the most widespread tools (also for decision-makers) to communicate with computers. The development of a system of voice recognition is still in progress although some devices are already in use.

In 1965, Lawrence Roberts and Thomas Merrill (both from MIT) successfully installed the first network between two computers. Connecting the TX-2 of the MIT with the Q-32 of the System Development Corporation (the first software company worldwide, located in Santa Monica, California, and originally part of the RAND corporation) they discovered that a simple connection between two computers was technically complicated. To resolve this problem in the future, Leonard Kleinrock's theories on data packets became an important part during the development process. Already in 1961 he had published his first thoughts about new forms of data transport within networks. In the beginning, his ideas were published in the technical report *Information Flow in Large Communication Nets* (RLE Quarterly Progress Report July 1961) and later became part of his PhD thesis at MIT in 1964 (Kleinrock 2007). Kleinrock came to the conclusion that an effective data transport has to take place in separate blocks: “(...) I was the first to introduce the idea of chopping messages into fixed-length blocks (...).” (Kleinrock 2008, p. 11). This idea, that was later called *packet switching*, turned out to become one of the underlying components of what later became the Internet.

At the end of 1966 Lawrence Roberts started working at ARPA where he continued his research on computer networks. In April 1967 he set up a meeting in which he explained to the principal investigators the necessity of a network called ARPANET which can be considered the origin of the Internet. One of his co-workers, Wesley Clark, suggested that to connect one computer (host) to such a network another computer would be necessary to function as a gateway. This was

considered necessary because of the lack of standardization among computers at that time. This gateway computer was called Interface Message Processor (IMP). IMPs were supposed to create a network of processors that were able to communicate with each other and at the same time communicate with the hosts connected to them.

3.1.2 NPL

In 1967 at the first ACM Symposium on Operating System Principles in Gatlinburg, Tennessee, Roberts presented the article *Multiple Computer Networks and Intercomputer Communication,* explaining the plan for ARPANET (Roberts 1967). Among the participants at that congress were also Donald Davies and Roger Scantlebury of the National Physical Laboratory (NPL) in the UK. Davies and Scantlebury, who at this symposium presented their work *A Digital Communication Network for Computers Giving Rapid Response at Remote Terminals* (Davies et al, n.d.) were also doing research on computer networks. Independently of the work done in the U.S. they had also developed the idea of sending data in separate packets (like Kleinrock) which they called *packet switching*. It was their research results that made ARPA adapt the expression of packet switching for their future work. In a conversation, the British investigators also informed Roberts about a third place that was doing research in the same area: the Research and Development Corporation (RAND).

3.1.3 RAND

RAND was founded in 1946 as a research project of the U.S. Air Force and in 1948 it was established as a non-profit research institute funded by the Ford Foundation. In the following decades it became one of the largest research institutes in the United States financed mainly by the U.S. government but also by the private sector, foundations and other governments contracting RAND for individual research projects. In 1962 a researcher at RAND, Paul Baran, started a project for the U.S. Air Force aiming at the development of a decentralized network to remain in control of

weapon systems (including nuclear weapons) after a hostile attack. In the same year he published his first findings about the advantages of decentralized networks being less vulnerable to external damages (Baran 1962). Two years later these and more findings towards communication networks were published in a further document called *On Distributed Communications* (Baran 1964). In these publications it became clear that Baran had a more military-oriented approach compared to ARPA researchers. Although ARPA's networking projects were financed by the U.S. Department of Defense their publications had a more civil character while Baran made clear already from the beginning that he was following a different line aiming at the defense of hostile attacks: “Let us consider the synthesis of a communication network which will allow several hundred major communications stations to talk with one another after an enemy attack.” (Baran 1964, p. 1). Following his theory a high number of nodes would be necessary to prevent the destruction of a communication system:

> We will soon be living in an era in which we cannot guarantee survivability of any single point. However, we can still design systems in which system destruction requires the enemy to pay the price of destroying n of n stations. If n is made sufficiently large, it can be shown that highly survivable system structures can be built -- even in the thermonuclear era. (Baran 1964, p. 16).

The investigations about systems of networks that happened at MIT, NPL and RAND were taking place independently from each other and all of them came to similar conclusions or complemented one another. In the end, the crucial approaches that let to the development of the Internet came from MIT and NPL. Baran's work at RAND is the reason why in the following decades the rumor kept going that the Internet was the result of a military project to control weapon systems during a potential nuclear war. In fact, Baran developed ideas of a communication network that would be able to survive a hostile attack. But it was a team of researchers at ARPA that in the end developed the network which later became the Internet. And although ARPA itself was officially connected to the Department of Defense the motivation of the MIT network researchers was of a non-military nature. Their objective was to create a network that facilitates researchers in several locations to access information of different institutions. In other words, they wanted to set up a new research tool to increase the distribution of knowledge:

> In June 1968, Roberts wrote an ARPA plan in which he proposed that ARPA build a working network that would permit researchers to log on to each other's computers over the network and gain access to the many

> resources of each computer. This plan was approved by Taylor [director of IPTO] in less than three weeks. (Kleinrock 2008, p. 12).

3.1.4 ARPANET

In January 1969 the company Bolt, Beranek and Newman (BBN) from Cambridge (USA) was authorized to develop the IMP for ARPA based on the Honeywell DDP-516 computer. The laboratory of Leonard Kleinrock, which at that moment had already moved from the MIT to the University of California in Los Angeles (UCLA), was chosen by ARPA to serve as the first node of the network, that is to say the first location where an IMP was going to be installed. To prepare this experiment Kleinrock set up groups of students at UCLA to be responsible for different aspects of the new network. In one of these groups which was involved in the development of network protocols two students called Jon Postel and Vinton Cerf were participating which in the following years took over important functions in the development of the Internet. Therefore, their roles will be discussed later in this text.

On 2 September 1969 the first IMP was connected to the SDS Sigma-7 computer at UCLA. One month later, a second BBN IMP was used to connect also the DEC 940 computer at the Stanford Research Institute (SRI) in Menlo Park, California. At that moment it was possible for the first time that two computers at far distant locations could communicate with each other. The first communication of this newly established ARPANET was the attempt of Kleinrock together with his students at UCLA to send the message “log” to SRI, expecting the DEC 940 to complete the message with the syllable “in”, forming the word “login”. Following Kleinrock,

> Charlie [a UCLA student] and Bill Duvall, the programmer at the SRI end, each had a telephone headset so they could communicate by voice as the message was transmitted. At the UCLA end, we typed in the 'l' and asked SRI if they received it; 'Got the l,' came the voice reply. We typed in the 'o' and asked if they got it and received 'Got the o.' UCLA then typed in the 'g' and asked if they got it, and the system crashed! (...) However, on the second attempt it worked fine! (idem, p. 13).

Until the end of the year also computers at the University of California in Santa Barbara

(UCSB, in November) and the University of Salt Lake City (Utah, in December) were connected to ARPANET. These four machines formed the beginning of the Internet. In the following years until 1975 several other computers at MIT, Harvard, BBN, Systems Development Corp, NASA, RAND, University of Illinois and others joined the network. Also other independently created networks joined ARPANET like the Alohanet of Norm Abramson (set up in 1970 and added to ARPANET in 1972) and the Packet Satellite Net (SATNET). SATNET became part of ARPANET in 1973 and represented the first international interface connecting the U.S. with the UK. At the same time (1972) Ray Tomlinson of BBN developed the most employed Internet application, the e-mail, which made short- and especially long-distance communication much easier than before. All important information related to new ARPANET applications were distributed by so-called *request for comments* (RFC). RFCs were and in the 21st century still are used as means of communication among Internet developers.

> … the normal cycle of traditional academic publication was too formal and too slow for the dynamic exchange of ideas essential to creating networks. ... These memos [RFCs] were intended to be an informal fast means of distribution for sharing ideas between network researchers. At first the RFCs were printed on paper and distributed via postal mail. As the File Transfer Protocol (FTP) came into use, the RFCs were prepared as online files and accessed via FTP. (Leiner et al 1997, p. 106).

The first RFC was published by UCLA student Steve Crocker on 7 April 1969 explaining the functioning of IMPs. In the following years all innovations like the protocols TCP, SMTP, FTP, HTTP and other topics were published and discussed in this way. Responsible for the publication of RFCs was the RFC-Editor which in the early years was Jon Postel and which today is a group of individuals within the Internet Society (ISOC). ISOC is a non-governmental organization founded in 1992 concerned with various issues of Internet development. It represents an important civil society actor within the Internet governance process and will be taken up later in this text. The publication of RFCs continues until today. All documents are available at the website of the RFC-Editor: http://www.rfc-editor.org. By December 2010 more than 6000 RFCs were published.

3.1.5 Internet Protocols

To enable computers to communicate in a network, protocols are needed. A protocol is a sequence of orders one or more computers are following automatically when requested. A

facilitated example of a protocol would be:

Table 3

Protocol		
Computer A		“Do you have the latest Amnesty International annual report?”
	Computer B	“Yes.“
Computer A		“Send me the latest Amnesty International annual report.”
	Computer B	*(sends the report)*
Computer A		“Do you have the 2005 Amnesty International anual report?”
	Computer B	“No.“
		(end of conversation)

To facilitate communication between computers of the ARPANET the Network Working Group (NWG), headed by Steve Crocker (who in 2011 became Chair of the Board of Directors of ICANN), developed the Network Control Protocol (NCP). In RFC 33 (published on 12 February 1970) Crocker, Jon Postel and Stephen Carr presented their ideas about the NCP. In this document they explained the communication problems occurring when computers of different types needed to be connected to each other in the same network like the ARPANET. The minimum the host computers had in common was not sufficient to build a stable network. To solve this problem was the objective of the NCP. In December 1970 it was installed on the first hosts and in 1972 all computers of the ARPANET were using the NCP.

In 1974 Robert Kahn and Vinton Cerf published their article *A Protocol for Packet Network Intercommunication* in which they explained the first steps of the Transmission Control Protocol (TCP), a new protocol that was going to replace the NCP in the future (Cerf; Kahn 1974). One reason for the development of the new protocol was the fact that the NCP included several problems. In RFC 801 Jon Postel summarized the situation referring to ARPA's research on different types of network communication as follows:

> It was clear from the start of this research on other networks that the base host-to-host protocol used in the ARPANET was inadequate for use in these networks. In 1973 work was initiated on a host-to-host protocol for use

> across all these networks. The result of this long effort is the Internet Protocol (IP) and the Transmission Control Protocol (TCP). (Postel 1981).

Both Kahn and Cerf had been involved in the development of computer networks and also in the ARPANET for years. The idea to develop the protocol came from Kahn who had worked at BBN before he joined ARPA. In 1973 he asked Cerf to participate in his project. Cerf had been involved in the formulation of NCP and because of this had in-depth knowledge about the details of that protocol. “So, armed with Kahn's architectural approach to communications and with Cerf's NCP experience, these two teamed up to spell out the details of what became the Transmission Control Protocol/Internet Protocol (TCP/IP).” (Leiner et al, 1997, p. 104). During the first steps of their project they developed the TCP and later when they discovered functional difficulties they split it up in March 1978 into two protocols: TCP and the Internet Protocol IP which were then joined together as the TCP/IP.

In the following years Kahn, Cerf and other researchers like Jon Postel tried to convince the ARPANET community that a complete transformation of all ARPANET computers from the NCP to the TCP/IP was necessary to create a stable and functioning network. In November 1981 Jon Postel presented a transition plan to all organizations involved in ARPANET. In this plan he explained the individual steps to be taken and also introduced a time schedule to realize this intent: “The goal is to make a complete switch over from the NCP to IP/TCP [sic] by 1 January 1983. It is the task of each host organization to implement IP/TCP for its own hosts. This implementation task must begin by 1 January 1982.” (Postel 1981). To underline the necessity of the transformation Postel and Cerf disabled the NCP protocol for one day in 1982 enabling only TCP/IP hosts to communicate with each other. Later the same year they repeated this process for another two days and emphasized that on 1 January 1983 the system would be changed completely to TCP/IP. In the same year when NCP was deactivated, a large number of organizations of military defense left ARPANET and founded the military network MILNET. “The transition of ARPANET from NCP to TCP/IP in 1983 permitted it to be split into a MILNET supporting operational requirements and an ARPANET supporting research needs.” (Leiner et al 1997, p. 105). TCP/IP remained the standard protocol of ARPANET and later the Internet.

3.1.6 DNS

In 1982 ARPANET consisted of about 250 hosts (Mueller 2002, p. 77). The majority of them was located in the USA and the rest in other Western European countries like France and the UK. All computers connected to ARPANET were using a file (hosts.txt) saved within their local systems to communicate with each other. This file included the names and virtual addresses of all computers of the network. As the number of hosts was steadily growing over the years it became obvious that a more efficient regulation had to be found. This problem was discussed by the ARPANET community through RFCs. In this context D.L. Mills of the technology developer Comsat Laboratories made clear that on the long run "it will not be practicable for every internet host to include all internet hosts in its name-address tables. Even now, with over four hundred names and nicknames in the combined ARPANET-DCNET tables, this has become awkward." (Mills 1981). Also David Clark of the MIT criticized the insufficiency of the then existing system to solve the problems of the future. Following his analysis, in July 1982 there were at most 25 active networks and a few hundred hosts. But for the future he saw a different scenario:

> The guidelines currently recommended are an upper limit of about 1,000 networks. If we imagine an average number of 25 hosts per net, this would suggest a maximum number of 25,000 hosts. It is quite unclear whether this host estimate is high or low, but even if it is off by several factors of two, the resulting number is still large enough to suggest that current table management strategies are unacceptable. Some fresh techniques will be required to deal with the internet of the future. (Clark 1982).

The same way Jon Postel confirmed that the old system based on a central data base that was duplicated by all hosts was not sufficient: "With the proliferation of networks and an accelerating increase in the number of hosts participating in networking, the ever growing size, update frequency, and the dissemination of the central database makes this approach unmanageable." (Postel; Su 1982). The first ideas for a new system which would be able to manage a larger number of virtual addresses was presented by Postel (who at that time was working at the Information Science Institute – ISI) and Zaw-Sing Su (SRI) in August 1982. In RFC 819 called *The Domain Naming Convention for Internet User Applications* they illustrated the concept of a new structure of the network which at that time they already called the Internet. One of the main innovations was the changing of names from simple constructions like ISIF to more complex versions like F.ISI.ARPA. In this new so-called tree-structure the last part (in the example mentioned: .ARPA) represented the

root, the administrative part. This way, a hierarchical system was created which became a fundamental part of the functioning of the Internet but also of its manipulation as will be shown in the later chapter on Internet filtering.

One year later, Postel presented a complete plan (including a time schedule) to implement the new system. A crucial difference of the new system compared to the old one was the absence of a list including the names and addresses of all hosts on each computer of the network. Instead of that, the new structure permitted all computers to send requests to the root servers each time they were looking for a specific address of another computer. In his plan, published as RFC 881 in November 1983, Postel was still talking about *domain style names*, an expression that was later changed to domain names: "Domain style names are being introduced in the Internet to allow a controlled delegation of the authority and responsibility for adding hosts to the system." (Postel 1983). He also introduced the expression *top level domains* (TLDs) defining the last part of a domain name (today: .com, .org, .net and others). As Postel had already announced in RFC 819 he confirmed also in his transition plan that the only TLD in the beginning of the new system would be .ARPA. But at the same time he underlined the intention to create more TLDs administrated by different organizations. The right to administrate a TLD was related to a number of conditions set up by Postel, including the necessity of a confidential and responsible person that was also able to resolve technical problems. Besides that a stable server of a sufficient size and a registration at the central authority were postulated. In his plan Postel did not define who the central authority would be and officially there was none at that time. But it was also obvious that he himself was a promising candidate.

In the two following RFCs (882 and 883), Paul Mockapetris (like Postel also from ISI) explained the structure of the new system and the function of a software he had developed and which would assist to set up the new domain system. Mockapetris underlined the impropriety of the old system which because of the centralization of host names in a table at the Network Information Center (NIC) was unable to guarantee functionality over the coming years with an increasing number of hosts added every month: "The size of this table, and especially the frequency of updates to the table are near the limit of manageability.", he wrote in RFC 882 explaining the necessity of a decentralized data base "that performs the same function, and hence avoids the problems caused by a centralized database." (Mockapetris 1983a). He introduced the concept of domain names which

was later called the Domain Name System (DNS) and which consisted of a hierarchy of servers. The DNS became responsible for translating names like unb.br to IP numbers like 164.41.101.38. Every computer (host) participating in the Internet (no matter if it is a server, a home computer or a mobile device) has an IP number to be identifiable to receive and send information.

To find the address unb.br a request (for example of a home computer) is send via a name server (in this case a provider) to a number of further hierarchically arranged name servers. The server on top of the hierarchy is the root server and is equipped with the information necessary to localize all existing TLDs (in this case the TLD .br). Starting from the highest level of the DNS (the root level) every name server is searching for the responsible server on the next lower level whose location will then be send to the requester (in this case the provider). In the first step the root server is informing the provider about the location of the server responsible for .br. This server is in turn equipped with the information regarding the location of the domain unb. So, the .br server is sending the respective information about the unb server to the provider which is then contacting the unb server and requesting the website unb.br. As a last step, the provider will send on the data from unb.br to the host (home computer) that initiated the request. This process takes place in a split second. To facilitate the whole action all servers save the information they received once in their cache memory so the next request can be answered immediately without contacting higher instances (which would cause web traffic and expenses).

During the first years of its existence the DNS consisted of 13 root servers worldwide of which 10 were installed in the USA, one in Japan, one in the UK and one in Sweden. In 2010 there were still 13 root servers, however most of them were distributed over several countries. This became possible due to the *anycast* technology which permitted to provide a higher quantity of servers with the same IP address. Nevertheless, the majority of the root servers remained in the USA and in Europe. Altogether there were about 200 servers in the root system in 2010 (13 plus x). As the number of operators remained 13 this is usually the official number mentioned for the root servers, which are denominated by the first 13 letters of the alphabet, A-M.

Figure 1: Root Server Locations 2010

Source: http://www.root-servers.org/

On top of the 13 roots is server A, administrated by VeriSign, the company that also became responsible for a number of TLDs, among them .com and .org, after it had acquired Network Solutions Inc. (NSI) in the year 2000.[17] Until then, NSI had been the original administrator of the first commercial TLDs. Root server A is the crucial network authority equipped with the root zone file, which contains the information regarding all existing TLDs on the Internet. In case of modifications of the root zone file announced by VeriSign, all other eleven operators have to copy the content of root A. This way it becomes obvious that the critical information concerning the DNS remains in the hands of a private company that at the same time is bound by contract to the U.S. Department of Commerce which needs to allow all changes made to the root zone before they can be implemented. Table 4 shows the 12 root server operators active in 2010 (one is responsible for two root servers).

[17] Network Solutions Inc. (NSI) was contracted by the DOC already in 1992 to manage crucial Internet resources like the root server A and the first TLDs .com, .net, and .org. Due to profitable perspectives of the TLD business, VeriSign (a U.S.-based e-commerce provider) bought NSI in May 2000. In 2003 VeriSign sold the registrar business of the NSI package to the investment company Pivotal Equity Group while remaining with the registry part. In 2007 another investment firm, General Atlantic, bought NSI. Since the acquisition, restructuring and selling by VeriSign, NSI functions as a registrar and service provider. The more profitable and influential part of the company (the registry sector) stayed with VeriSign.

Table 4

Root Server Operators 2010		
Root Server	**Operator**	**Sector**
A	VeriSign	private company (USA)
B	USC-ISI	University of Southern California – Information Science Institute Institute (USA)
C	Cogent Communications	private company (USA)
D	UMD	University of Maryland (USA)
E	NASA	National Aeronautics and Space Administration (USA)
F	ISC	Internet Systems Consortium, private company (USA)
G	DOD	Department of Defense (USA)
H	ARL	U.S. Army Research Laboratory (USA)
I	Netnod	Non-profit organization, Sweden
J	VeriSign	private company (USA)
K	RIPE	Réseaux IP Européens Network Coordination Centre (Netherlands)
L	ICANN	Internet Corporation for Assigned Names and Numbers (USA)
M	WIDE	Widely Integrated Distributed Environment, research project at Keio University, Japan

Source: http://www.root-servers.org/

3.1.7 IANA

At the time the DNS was established the Internet did not have a major impact on governments, companies or the population in general. It was a network set up and run by people which were motivated by a certain form of idealism and a vision to develop a service that in the future would facilitate access to information for the largest amount of people possible. The commercialization of the Internet was no objective. The question of regulation of and authority over the root server system and the TLDs did not cause particular dispute. As the DNS and the first TLDs were created by researchers at the ISI there was a certain consensus among the participants of the network that people at the same institution were responsible for the central parts of network

administration. The person who was taking the respective decisions at ISI was Jon Postel. The first TLDs created by Postel were *generic top level domains* (gTLDs, e.g. .com, .net, .org) and country code top level domains (ccTLDs , e.g. .br, .ar, .cl). Due to the increasing number of TLDs there are more sub-categories for gTLDs today like *sponsored top level domains* (e.g. .jobs or .museum), *generic-restricted top level domains* (e.g. .biz or .name) and *infrastructure top level domains* (e.g. .arpa). In October 1984 Postel presented via RFC 920 the first TLDs .com, .edu, .gov, .mil, .org and in January 1985 also .net (Postel; Reynold 1984). Besides that, he announced the creation of ccTLDs based on the ISO-3166 list of the International Organization for Standardization. The administrative function Postel created this way was called *Internet Assigned Numbers Authority* (IANA) and received an institutionalized character in 1988 when ISI was contracted by the U.S. Department of Commerce (DOC) to manage the DNS until 1997 (Mathiason 2009, p. 50). Because of this function and his personal dedication for the Internet Postel gained an enormous reputation within the Internet community of researchers and engineers. This way a personalization of IANA was happening which resulted in a number of conflicts with other actors (especially from the private but also from the public sector) which were going to enter the scenario in the following years.

The personalization of IANA underlines again the informal character of the Internet during the time before its commercialization. One example for this is the delegation of TLDs by Jon Postel which was done without any strict regulations. He simply chose the individuals in a first come first serve manner, in which the candidates only had to show a low quantity of qualifications like responsibility and technical know-how. Besides the ISI also the Stanford Research Institute (SRI) played in important role in the technical regulation of the Internet. Since 1971 the SRI was controlling the original hosts.txt file which contained all addresses of computers taking part in the network.

When the DNS was introduced (making hosts.txt obsolete), the SRI maintained its crucial position by controlling the root server A and the TLDs .com, .org and .net. Following Mueller:

> The services were performed under contract to the Defense Communications Agency and given the title Defense Data Network-Network Information Center (DDN-NIC). As domain style names were introduced, the SRI-operated DDN-NIC retained its familiar role as the central point of coordination for the name space. It became the 'registrar of top-level and second-level domains, as well as administrator of the root domain name

> servers'... In November 1987, SRI's DDN-NIC also took over the IP address assignment and registry function from Postel... (Mueller 2002, p. 82).

As the SRI had always been a “friendly, non-profit, and effectively passive partner” (Goldsmith; Wu 2006, p. 35) cooperation between the institute and Postel was working without any difficulties. This changed when in 1990 the contract between SRI and DOC ended and through an open bidding the private company Government Systems Inc. gained the new contract in 1991 which it then delegated to the smaller company Network Solutions Inc. (NSI). At that moment the first actor from the private sector took over a crucial part in the process of Internet regulation. NSI started controlling root server A and the most important TLDs like .com, .net and .org (besides others).

3.2 ISOC and the Memorandum of Understanding

The development of HTML and the first browser by Tim Berners-Lee in the beginning of the 1990s opened up the possibility for more people to participate in the Internet. In the first years the community of Internet users was made up basically of researchers and engineers who were in the first place interested in setting up an open network on a non-commercial basis. The commercialization of the Internet changed this original scenario and opened the door for enterprises and investors which regarded the Internet as a new business opportunity. NSI was the first one to prove the financial potential of the Internet by starting to charge 50 U.S. dollars of each person ordering a domain. Until that day they had received one million U.S. dollars from the American government to fulfill their obligations concerning the root zone file. After NSI started charging every individual client the company had an annual growth rate of more than 100% doing a disproportionately high profit as can be seen in the following example. While in 1992 there were 300 new domain registrations per month this number increased up to 45.000 per month in 1995. In 1996 there were 637.000 domains registered (Mueller 1999, p. 500).

This way NSI was able to make millions of dollars in about five years. Impressed by these numbers and the potential for further economic growth, more companies (both recently founded and

established ones) entered the market as providers or e-commerce entrepreneurs. Summarizing the development of those years, Leonard Kleinrock explained the antagonism between the members of the early Internet community and the private sector:

> One should note that the culture of those early days of the ARPANET community was one of open research, shared ideas and works, no overbearing control structure, and trust in the members of the community....We felt strongly that control of the network should be vested in all the people who were using the net and not in the carriers, the providers, or the corporate world. (Kleinrock 2008, p. 12).

The most important attempt of researchers and engineers to maintain control over the Internet was the formation of the Internet Society (ISOC) in 1992. One central actor in this context was Vinton Cerf. Cerf played an active part during the incorporation of the Internet Architecture Board (IAB) into ISOC. The IAB (formerly known under different changing names since the 1980s) was supposed to take over decisive aspects of Internet regulation. After the foundation of ISOC, the IAB was incorporated into the new organization as a technical advisory group (Mathiason 2009, p. 32f). The first official member of ISOC was Jon Postel. In fact, Cerf and Postel were both accompanying the development of the Internet since the early days and both frequently had important positions in its context. Furthermore, they both symptomatically stand for different streams of thinking in the history of the Internet.

Postel and Cerf already went to the same high school on San Fernando Valley (Van Nuys High) in California but met each other only at UCLA working for ARPANET (Cerf 1998). Although they were sharing the same ideas concerning the non-commercial character of the Internet they were also following profoundly different approaches about how to realize this undertaking. While Postel was following a way that was based on his authority as a person and the respect that he received within the Internet community Cerf was more pragmatic and rule-oriented. Different than Postel, Cerf accepted the increasing influence of the U.S. government on the Internet. At that time Washington was aiming at not letting the Internet community alone decide about the administration of the network.

Nevertheless, ISOC's objective was to replace the U.S. government as the highest authority on the Internet. Not just to reduce an increasing influence of the private sector (which was supported by Washington) but also because the originally small network of a few dozen North American institutions had grown and had become an international phenomenon which could not be controlled by a single government.

The economical success of NSI was not only one of the reasons why the Internet community decided to bundle its forces inside the Internet Society, it was also a driving impulse for ISOC to develop a new scheme of Internet administration before the contract between NSI and the DOC was going to end in 1998. To realize this intention ISOC started looking for influential partners like intellectual property organizations. Those actors had already shown concern for a few years about the uncontrolled and growing market of Internet names. As they were aspiring a regulated manner for the acquisition of protected names a cooperation with ISOC was a promising option. Members of the World Intellectual Property Organization (WIPO) and the International Trademark Association (INTA) participated in the International Ad Hoc Committee (IAHC), a group that was set up by ISOC to develop the structures of a future authority over names and numbers and the root system (Franda 2001, p. 50). Besides representatives of intellectual property groups there were members of different other organizations like IBM, the International Telecommunications Union (ITU) or the Internet Engineering Task Force (Mueller 2002, p. 143). Unsurprisingly, NSI was not invited to participate in the debates, although it was playing a major role at that time. The reason for this decision was the fact that NSI (as the main commercial actor and contractual partner of the U.S. government) was not considered a possible partner but an opponent of the Internet community. Nevertheless, the public sector also had a representative in the IAHC: George Strawn was invited to join the group as a member of the National Science Foundation (NSF) which at that time still held an important position due to financing of the backbone infrastructure.

Between 1994 and 1998 there were four attempts to take away control over the root server A from NSI. The first one in 1994 aimed at transferring the authority over IANA to ISOC. This idea was brought up mainly by Jon Postel and can be seen as a step towards privatization of IANA. In July 1994, Postel developed the first proposal to realize the transfer (Mueller 1999, p. 500). It did not get the necessary support and so the aspired change did not happen. However, the U.S. government realized that the situation of the DNS caused growing dispute and therefore

Washington started its own debate about who had the necessary authority to administrate the Internet. Following Milton Mueller there was no clear response regarding this question at that time: “Clearly, ISOC was attempting to assert ownership of the name and address space via its control of IANA. Just as clearly, it had no legal basis for this assertion. But if ISOC and IANA did not own it, who did? The question was left unanswered at the time.” (Mueller 1999, p. 500).

The second attempt was motivated by the perception of Postel and other ISOC members that NSI was making enormous profits through the commercialization of TLDs. On the one hand the financial benefits stood in contrast to the ideals of the Internet community to create a non-commercial and open knowledge network. On the other hand Postel realized that those gains could be used to finance ISOC and the administration of the Internet. Following this logic the introduction of new TLDs could be useful to weaken NSI's monopoly and to resolve the financial question of ISOC at the same time (idem). For this reason Postel suggested the creation of 150 new TLDs in September 1995. To decentralize but still control the domain market, those companies administrating new TLDs would have to pay an annual fee of 2.000 U.S. dollars to ISOC plus another 2% of profits made with TLDs. But also this second attempt did not work out. Besides the private sector (which criticized the payment system) and the International Telecommunications Union (which wanted to take part in the administration of the Internet), especially intellectual property rights organizations did not agree with the creation of a large number of new TLDs. 150 new domain names meant as well an oversized threat to their pressure group. To bring together the different perceptions on the issue at hand, Postel, Cerf and other members of ISOC decided to start another attempt and to include more stakeholders into the whole process.

This third effort was the most elaborated and was realized by the IAHC. After three months of negotiations the group presented a final report in which it explained its proposal for a new structure of Internet administration (IAHC 1997). IAHC wanted to create a non-profit monopoly of TLDs. This way, all TLDs were supposed to be included into one central data base to which all registered providers would have access. This idea was quite different from what Postel had suggested before when he tried to split up TLDs among providers instead of creating a pool for everyone. IAHC furthermore considered concerns of intellectual property rights stakeholders by reducing the number of new TLDs to seven. Besides that, a time frame of 60 days was going to be set up to settle intellectual property rights issues before new TLDs were going to be offered

publicly on the market. The new regulations were written down in the Generic Top Level Domain Memorandum of Understanding (gTLD-MoU, also known as MoUvement or simply MoU). The MoU was signed by Postel and ISOC President Don Heath on 1 March 1997 in Geneva. It confirmed the beginning of the registration process for new TLDs in January 1998. Following Heath, the U.S. government had no choice but to accept the MoU as the IAHC and ISOC had control over the domain name administration via IANA (CNET 1997).

To arrange the registration of TLD providers the new governance concept envisioned the creation of the Council of Registrars (CORE), a non-profit entity installed in Switzerland. Interested providers would have to pay an entrance fee of 20.000 U.S. dollars, a monthly contribution of 2.000 U.S. dollars plus fees for TLD registrations. In the following months after the MoU was signed, CORE received about one million dollars from several organizations interested in the new TLDs (Mueller 2002, p. 165). Obviously, NSI became worried because of this development and started lobbying against the MoU (idem, p. 147). And Washington answered.

While in the years before, the failed attempts of Postel and ISOC called limited attention of the U.S. government, the MoU changed this situation and brought the debate on Internet regulation to a higher level. “The controversies generated by the gTLD-MoU (...) and the impending expirations of IANA's funding and the Network Solutions Cooperative Agreement forced the federal government to either yield or assert responsibility.” (Mueller 2002, p. 154).

A central person representing the U.S. government's interests in this situation was Ira Magaziner. Magaziner became an advisor for the Clinton administration after he had worked as a business consultant for the Boston Consulting Group and other global companies. Before he became involved in Internet policy debates, Magaziner was a key figure in President Clinton's health care reform project in the USA in 1993-1994. The project, which was lead by then First Lady and later Secretary of State Hillary Clinton, was unsuccessful due to opposition by Republicans and the health care industry. At that time Magaziner obtained the reputation as a pro-regulation professional which caused doubts among several actors in the IT policy debates when he was declared responsible for the U.S. government's IT policy strategy in December 1995 (Broder 1997).

However, in the following months Magaziner made clear that he was not in favor of creating public regulatory mechanisms. He developed the U.S. Administration's Framework for Global Electronic Commerce in which was pointed out that self-regulation was the key for a successful development of the Internet (The White House 1997). Magaziner tried to ensure transparency during the drafting process by including several actors from the private sector, civil society, the Internet community and academics in the debate. Besides that, a draft was available on the Internet for public comments. The final version, which was published on 1 July 1997 by President Bill Clinton and Vice President Al Gore, included five leading principles: 1) The private sector should lead. 2) Governments should avoid undue restrictions on electronic commerce. 3) Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce. 4) Governments should recognize the unique qualities of the Internet. 5) Electronic commerce over the Internet should be facilitated on a global basis (idem).[18]

These principles underlined the character of the document, aiming at creating space for economic development in the IT sector. At the time the framework was published, e-commerce was still in its early stages. Although pioneers like eBay Inc. and Amazon.com Inc. were already on the market, electronic commerce still needed its basic infrastructure like online payment systems and other applications to be developed. Magaziner recognized the potential that e-commerce could mean to the economy of the U.S. and other states. The decision of the Clinton Administration to refrain from market regulation can therefore be seen as a crucial step to Internet growth.

By getting involved further into IT policy debates, the U.S. government also pretended to inhibit the gTLD-MoU. Magaziner's objective was not only to reduce U.S.-governmental influence in Internet regulations but also to avoid any government to take control over the root server system. The fact that Postel was about to create an organization based in Switzerland in which not only ISOC but also the ITU was going to be involved concerned the U.S. government. Following their point of view, the involvement of an international organization could cause growing influence of its member governments. However, political debates in the U.S. at that time proved that critics of the MoU were not only skeptical about governmental influence in general but particularly about

[18] Ten years after the framework was presented, Scribe Media published a video of Ira Magaziner recorded in 2007, reflecting on the process of development of the document and its impact. The video is available online at http://www.scribemedia.org/2007/07/18/magaziner/

influence of other governments than the U.S. Administration (Goldsmith; Wu, p. 41f). On the other hand, although Washington claimed to refrain from governmental Internet regulation several actors (governmental and non-governmental) from different countries kept on criticizing the strong position of the U.S. in global Internet governance affairs.

The dispute about the MoU showed already in the early stages of Internet governance, that a lot of different stakeholders were interested and became involved in Internet regulation. And at the same time it exemplified that being part of a certain stakeholder group did not necessarily mean having the same interests. Especially in the private sector it became obvious that economic interests of those already profiting from the early growth in the e-commerce industry did not match with those who were willing to participate in the same business area. While Network Solutions was heavily lobbying against the MoU, as one of the memorandum's aims was to break its monopoly on certain TLDs, a great number of other companies from the telecommunication and IT sector favored Postel's plans. They expected to become part of a growing and profitable IT sector in the coming years. Especially companies from outside North America were eager to invest in what was mostly seen as a U.S. dominated market. However, other actors from the private sector like IBM and AT&T opposed the MoU due to lack of trademark protection (Mueller 2002, p. 151).

When in January 1998 new TLDs were supposed to be added to the root server system NSI was still opposing the authority of IAHC and the MoU. Beyond that the company had strict orders from the NSF and also from Ira Magaziner as a representative of the U.S. Administration to not include any new TLDs to the system. NSI was a crucial actor in this question because it was in control of the root server A, the central server of the Internet. In the hierarchical system of the DNS, root server A was the highest authority where other servers were sending their requests to translate domain names into IP numbers. To include new TLDs the central root server had to be manipulated. As this was not going to happen, Postel changed his plans. Instead of adding new TLDs to root server A where all secondary root servers were getting their information from, he decided to redirect the secondary servers and thereby create a new root server A under his control. For this procedure he chose the IANA server, located at the University of Southern California, to be the new root server A. This episode in the history of the Internet, which lasted only a few days, shows the personal character that the Internet still had at that time. The redirection of the secondary root servers had to be arranged by the respective operators, which happened to be individuals who all

knew and respected Postel for his efforts and dedication regarding the Internet (Castells 2001, p. 31). When Postel asked them in an e-mail on 28 January 1998 to redirect their servers away from NSI and towards IANA, eight of twelve secondary root servers, located at universities and research institutions, followed Postel's request (Goldsmith; Wu 2006, p. 44). The other four were not asked as they were being controlled by the U.S. government and therefore contrary to Postel's and the IAHC's policy plans in general.

The manipulation of the root server system was a technical break of the Internet. At that time it was possible to split the Internet into two networks with different domain name systems, one controlled by the U.S. government and a second one controlled by IANA and the IAHC. There were two main reasons why nothing seriously happened to the Internet on that day and especially why Internet users were not affected by the redirection. The first reason is that Postel was willing to demonstrate his technical authority (especially towards NSI and the U.S. government) but was not willing to harm the network itself. To manage the continued functioning of the Internet he redirected the IANA server to NSI's official root server A. By doing so he ensured that all networks were continuously working as before, getting their requests answered by the DNS file on the NSI server. Technically NSI was still in power but IANA was recognized by the majority of the root server operators as an approved authority.

Postel's action called the attention of the U.S. government only few hours after he managed to redirect the secondary root servers. Ira Magaziner, who at that time was attending the World Economic Forum in Davos, immediately took action when he got informed about the occurrences (idem, p. 45). By making pressure on Postel together with a representative of the University of Southern California, Magaziner achieved to reestablish the status quo of the root server system. All secondary root servers were directed back to NSI. After this episode the U.S. Administration never let go of the root server A.

Root server A continued with NSI and later VeriSign. VeriSign continued close cooperation with the U.S. government to control the server. Today, the two servers operated by this private company from Dulles in the state of Virginia, are considered “national IT assets by the Federal U.S. government” (VeriSign n.d.). Besides that, the U.S. Administration has a direct influence on changes of the root server system as the U.S. Department of Commerce is the responsible authority

to instruct VeriSign about changes in the root zone. Another decisive institution in this process is the Internet Corporation for Assigned Names and Numbers (ICANN) which was founded in 1998 and whose function will be analyzed in the following paragraphs. The relation between the U.S. government and VeriSign was consolidated in March 2011 when the company became responsible for the administration of the governmental TLDs .gov and fed.us (Marsan 2011).

3.3 ICANN

3.3.1 Green Paper

In April 1997 the U.S. government set up an interagency working group under the chair of the Office of Management and Budget (OMB) and the Office of Science and Technology (U.S. House of Representatives 1997). Under its chairs Brian Kahin and Becky Burr this Interagency Working Group on Domain Names was preparing policy advices for the Clinton administration to deal with the complicated situation the Internet was confronted with. The members of the working group came from a variety of governmental agencies, among them the National Science Foundation, NASA, the Department of Commerce (DOC) and the National Telecommunications and Information Administration (NTIA) (NSF 1997). The common denominator of the working group's members was the opposition to the governance structure that the IAHC was trying to establish.

During the process of development of what later became known as the Green Paper, NTIA and the DOC were looking for contributions by a large number of actors involved in Internet policy debates. For this reason NTIA set up a list of questions entitled as Request for Comments on the Registration and Administration of Internet Domain Names which was published on 2 July 1997 (NTIA 1997d). This date can be seen as a strategical decision as on the day before, President Clinton had presented the Framework for Global Electronic Commerce, also known as the Magaziner Report. That document had already made clear which direction the government was going to take in the following months. And the Green Paper was going to be a next step in the same direction of privatization of the root zone and DNS administration without giving up completely

political control over it. In the Request for Comments, NTIA asked all interested actors and individuals to send in "comments on the current and future system(s) for the registration of Internet domain names." (idem). This step was taken to get the opinion of those who were for years involved in Internet issues but also to create a certain transparency during the whole process which in the end would lead to a final governance framework which would affect all Internet actors worldwide. So it was both knowledge and legitimacy that NTIA was looking for. As stated before, the U.S. government wanted only a minimum of regulation, but they also wanted to be the one to define this minimum. They had no interest at all in handing over complete control over the root server system and the DNS to other actors, especially other governments. As the situation was tense due to confrontations between Washington and a great number of Internet actors, Magaziner tried to include as many as possible of those actors in the new process. An ongoing confrontation would have weakened the Internet for a long period of time and therefore reduced trust and investments in the network. And for Magaziner, economic growth in the e-commerce sector was one of the central aspects of his motivation.

The Request for Comments included a short introduction to the problem at hand before presenting a list of six principles which were supposed to build the foundation of the Green Paper. The principles were:

> a. Competition in and expansion of the domain name registration system should be encouraged. Conflicting domains, systems, and registries should not be permitted to jeopardize the interoperation of the Internet, however. The addressing scheme should not prevent any user from connecting to any other site.
> b. The private sector, with input from governments, should develop stable, consensus-based self-governing mechanisms for domain name registration and management that adequately defines responsibilities and maintains accountability.
> c. These self-governance mechanisms should recognize the inherently global nature of the Internet and be able to evolve as necessary over time.
> d. The overall framework for accommodating competition should be open, robust, efficient, and fair.
> e. The overall policy framework as well as name allocation and management mechanisms should promote prompt, fair, and efficient resolution of conflicts, including conflicts over proprietary rights.
> f. A framework should be adopted as quickly as prudent consideration of these issues permits. (NTIA 1997d).

Following the list of principles a catalog of 28 questions was posed, categorized in four sections: 1) general/organizational framework issues, 2) creation of new gTLDs, 3) policies for registries and 4) trademark issues. In the next approximately six weeks that were allocated to respond, NTIA received 432 reactions (some of them after the closing date). It is interesting to mention that the first 17 comments arrived already on 1 July, the filing date of the Request for Comments, although the official date of publication in the Federal Register was 2 July. The reactions that arrived on an almost daily basis were of different nature. While some originated from users who presented for example problems with TLD registering processes others deeply discussed serious issues regarding the underlying policy process. Mathiason and Kuhlman (1998) took a closer look at the comments and came to the conclusion that out of 432 comments 150 did not match the necessary standards to be analyzed because they were: 1) part of a petition favoring the suggestions of the private company pgMedia, 2) duplicates, 3) without information, 4) not reported online. The remaining 282 comments were categorized into groups of senders. The majority of comments was sent in by individuals (52,8%). The rest came from small businesses (14,9%), web managers (13,1%), business associations (5%), ISPs (4,6%), large corporations (4,3%), NGOs (3,9%), international organizations (0,8%) and governments (0,7%). 93% of them all came from within the United States. Among the remaining seven percent 5,6 were sent from English-speaking countries like Canada, the UK, and Australia.

In the following paragraphs three major issues will be discussed that were addressed in a number of comments or that treated crucial issues for the future of the Internet: 1) the trademark debate, 2) the TLD debate and 3) the Internet Protocol debate.

The first two debates are to some extend closely linked to each other. This happens because the TLD debate includes both the question of which new TLDs were to be launched and who had the right to own them. As one commentator stated: “Every time you add a gTLD, you add another potential battleground for companies to fight over the rights to a domain name, and another potential domain name that can be hijacked away from its rightful owner.” (NTIA 1997b). Furthermore the same commentator made clear that there was an international dimension to this issue. In a growing global e-commerce market, TLDs had to be distributed in a way that not only U.S.-American ownership would be respected: “All trademarks should be given weighting when considering domain name disputes, IRRESPECTIVE of the country of origin of the domain name.

This is vitally important: U.S. trademarks should not be given any kind of precedence over trademarks issued by other countries.“ (idem).

Dennis Fazio, Executive Director of the IT company Minnesota Regional Network identified three main problems that the new regulation would have to solve. Following his analysis, all other major problems were based on these three issues: 1) demand by several parties for the same name, 2) use of the domain name system as a directory service and 3) technical and operational management of the growing Domain Name System and in fact all going back to one highly discussed issue at that time: the question of trademarks (NTIA 1997a). The constant debate on this concern later resulted in ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) (Froomkin 2002).

Other comments referred to the question of TLD structures and the debate about if, how many and which new TLDs were to be released. Some debated a number of new TLDs like .store, .rec, .nom, .web, .firm, .inc, or .ltd. (among them comments no 159, 235, 286[19]). In this debate it became obvious that a number of commentators was not aware of the international character of the Internet or that they were following a U.S.-centric point of view. Therefore certain TLDs like .inc or .ltd were not very promising as they referred to the North American context only or (in case of .ltd) to a limited number of other countries like the UK and some former British and German colonies. Following this logic an enormous number of other TLDs would have to be introduced to cover several types of legal entities in countries all over the world. The same can be mentioned regarding the suggested introduction of U.S.-centric governmental TLDs like in comment 109. The creation of TLDs referring to U.S.-American states like .ca for California (as suggested by the commentator) would not only cause a dispute with the state of Canada to which .ca was connected but also required the creation of a few hundred TLDs for legal territories and federal states in several countries. In fact, the number of TLDs remained an important issue over the years. In 2010 there were more than 300 top level domains available, most of them ccTLDs.

Regarding the Internet Protocol question, Jesse Kornblum, who at that time was a Computer Science student at the Massachusetts Institute of Technology, mentioned another point which was not considered a crucial problem in 1997, although already back then it was obvious especially to

[19] All comments can be accessed at: http://1.usa.gov/w2HDZg.

IT engineers that this issue would call more attention in the near future. Kornblum stated: "It may very well be necessary to expand IP addresses to five blocks. (Each block can range from 0-255). Having existing systems work with these new systems would require updating the Internet, a daunting task, but nonetheless necessary..." (NTIA 1997c). The problem that Kornblum was referring to was the limitation of IP addresses. The IPv4 system that was used at that time offered a limited number of about 4,3 billion IP addresses. In the early 90s this was not a serious problem but with the growing number of computers connecting to the Internet the stock of IP addresses was diminishing. When in the early 21st century a growing number of new IT devices (like smart phones and others) required their own IP address, the debate on the follow-up of IPv4 called the attention of a wider audience. However, not five blocks as Kornblum suggested in 1997 were going to be implemented in the new protocol version, but eight. This new protocol called IPv6[20] was introduced already in 1998 through RFC 2460 by some of the developing engineers (Deering; Hinden 1998). It offers about 340 undecillion IP addresses.[21] About two years later, the first policy makers started putting the topic on their agenda. DeNardis explained in *Protocol Politics – The Globalization of Internet Governance*:

> Beginning in 2000, governments in Japan, Korea, China, India, and the European Union established national strategies to upgrade to IPv6. These governments have designated the new protocol as a solution to projected address shortages and also as an economic opportunity to develop new products and expertise in an American dominated Internet industry. In contrast to international address scarcity concerns, U.S. corporations, universities, and government agencies have historically possessed ample IP addresses. The United States, with abundant Internet addresses and a large installed base of IPv4 infrastructure, remained relatively dispassionate about IPv6 until discussions commenced in the area of cybersecurity and the war on terrorism after the terrorist attacks of September 11, 2001. (DeNardis 2009, p. 17).[22]

[20] IPv5, officially known as the Internet Stream Protocol and later Internet Stream Protocol Version 2 or ST2, had an experimental character and did not come into effect but was later replaced by IPv6. More details on ST and ST2 can be found in RFC 1190 and RFC 1819.

[21] For better understanding: one undecillion has 36 zeros.

[22] In February 2011 ICANN officially declared the end of the IPv4 stock by handing over the last addresses to Regional Internet Registries (RIR) (Lawson 2011). Some leading Internet companies like Facebook, Google and Yahoo declared to start testing IPv6 on a larger scale on 8 June 2011, which for that reason was called World IPv6 Day.

After considering the reactions to the Request for Comments, the U.S. government published the Green Paper on 30 January 1998.[23] The complete title of this document was *A Proposal to Improve Technical Management of Internet Names and Addresses, Discussion Draft 1/30/98* (NTIA 1998a). A second (final) version with an additional introduction was published on 20 February 1998 in the Federal Register (DOC 1998a).

In the Green Paper the U.S. government explained the status quo and their future plans for governing the DNS and the root server system. Their principle goal was to establish a non-profit corporation until 30 September 1998 without direct governmental control (which in the end was bound to the U.S. Department of Commerce). Also in relation to the root server system there was no doubt about a strong U.S. influence. In fact, this special relation between the U.S. and the central organizations and companies controlling the root and DNS became a problem for many actors involved in Internet policy debates in the following years. The dominant influence (directly and indirectly) of the U.S. government caused strong criticism in relation to the governance model. In the Green Paper the U.S. Department of Commerce openly stated:

> Currently, NSI operates the "A" root server, which maintains the authoritative root database and replicates changes to the other root servers on a daily basis. Different organizations, including NSI, operate the other 12 root servers. In total, the U.S. government plays a direct role in the operation of half of the world's root servers. (idem, p. 8826).

Furthermore it was said:

> The U.S. government would participate in policy oversight to assure stability until the new corporation is established and stable, phasing out as soon as possible and in no event later than September 30, 2000. The U.S. Department of Commerce will coordinate the U.S. government policy role. [...] … the new corporation will be headquartered in the United States, and incorporated under U.S. law as a not-for-profit corporation. It will, however, have and report to a board of directors from around the world. (idem, p. 8828).

Four principles were mentioned to be considered during the development process of the new governance system: stability (both technical and organizational), competition to enhance innovation, private/bottom-up coordination (instead of governmental control), representation

[23] This was two days after Jon Postel managed to switch root A from NSI to IANA.

(regarding the diversity of the user community). Also trademark issues were treated as an important aspect. In this context the Green Paper suggested the installation of data bases to facilitate access to certain personal data of domain owners in case of trademark problems. Today in deed any Internet user can access these data (in most cases) openly on the Internet using several “whois“-data bases.[24] Besides that the document also addressed the controversial topic of new TLDs by trying to find a compromise between supporters and opponents of new domains:

> The number of new top-level domains should be large enough to create competition among registries and to enable the new corporation to evaluate the functioning, in the new environment, of the root server system and the software systems that enable shared registration. At the same time, it should not be so large as to destabilize the Internet. (idem, p. 8829).

The debate on TLDs was also reflected in a number of comments that the DOC received after the Green Paper was published. In several cases commentators suggested a number of new TLDs to be created. Among them were .service (for service websites), .ind (for independent users) and .fun (for games and entertainment). Also the creation of TLDs based on company names was discussed. However, this proposal would have caused enormous administrative difficulties considering the number of companies existing all over the world. Besides that it could have caused a serious trademark problem as especially smaller companies' names appear in several countries at the same time. For this reason, larger corporations like Disney, Viacom and AOL demonstrated their concern about the creation of new TLDs and registries (organizations responsible for the administration of TLDs). Jake Winebaum, then President of Disney Online, criticized the idea of installing competing registries which would have caused serious problems to trademark owners. Instead, he favored the centralized model of CORE, proposed by Postel and the the Internet Society (DOC 1998b). Viacom's representatives declared even the creation of a small number of five new TLDs as a “significant threat to trademark owners“ and asked for a “single administrative dispute policy“ instead of a decentralized system of dispute policies set up by individual registries (DOC 1998c). Also AOL (at that time the biggest online provider worldwide) underlined the importance of trademark issues and favored parts of Postel's model of the gTLD-MoU (DOC 1998d). In fact, not only the comments of larger enterprises but the general debate and participation of smaller companies, actors and individuals resulted in a different picture than Mathiason and Kuhlman had analyzed during the earlier RFC process.

[24] Although this might not be the exact kind of data base trademark protectors were looking for at that time.

This time about 20% of the comments came from outside the US, compared to only 7% during the RFC process. Among those international participations were especially people from institutions (like international organizations), private companies and civil society. Therefore it was a larger diversification among different stakeholder groups and less individual contributions. The broader approach of the actors involved in the debate caused a professionalization of the debate. The fact, that the percentage of international contributions had grown showed, that Internet regulations were increasingly seen as a global and not exclusively a national policy issue. It can also be argued that a growing number of actors tried to avoid in the last minute that one single country decided on the future of a worldwide information network. Therefore, U.S.-centric orientation of the debate was one of the main aspects to be criticized, by both U.S.-American and international contributers. Especially non-Americans favored an international solution. But also 40% of U.S.-American debaters mentioning the international approach favored it while less than 5% spoke out against it.

3.3.2 White Paper

Two and a half months after the end of the period to comment on the Green Paper the NTIA published the White Paper, officially titled as “Management of Internet Names and Addresses“ (NTIA 1998b). The White Paper is known as the crucial document based on which ICANN was founded in October 1998. It was categorized as a statement of policy by the U.S. government and was based on the content of the Green Paper and the comments the DOC had received. It furthermore mentioned the MoU and the IAHC initiative as a part of the development process concerning DNS regulation. This can be considered a step towards the supporters of that earlier governance model which a few months before was still heavily criticized by the government. The large number of comments supporting the IAHC model or part of it, lead to a reconsideration by the DOC to create a model that would include as many interest groups as possible and therefore stabilize the DNS system and the Internet for the coming years. Slavka Antonova, member of the Steering Committee of the Global Internet Governance Academic Network called the White Paper a “surprisingly open approach to DNS management privatization“ (Antonova 2008, p. 156).

The White Paper picked up the four principles of the Green Paper, being stability, competition, private bottom-up coordination and representation. There was a wide agreement among most commentators that these principles were to be supported. In some cases, civil society actors asked for the inclusion of additional principles regarding human rights protection and freedom of speech. However, the DOC declared, that the U.S. government policies were focused on DNS management only. This merely technical issue did not interfere with human rights and therefore (following the DOC) did not need a special inclusion of principles regarding human rights.

The White Paper furthermore mentioned four central functions of the DNS system that were defined during the Green Paper process and presented them with a few adaptations based on the debate with several stakeholders. These functions were: 1) To set policy for and direct the allocation of IP number blocks; 2) To oversee the operation of the Internet root server system; 3) To oversee policy for determining the circumstances under which new top level domains would be added to the root system; and 4) To coordinate the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet (NTIA 1998a, p. 8828). However, the DOC disapproved the demand for the creation of two separate bodies to administer Internet names and numbers. For organizational and also financial reasons it insisted on the constitution of a single body to accomplish both of these tasks together. This body was planned to be created as a private not-for-profit corporation within the United States. Following the DOC the U.S. was the most appropriate place for the establishment of this new organization, especially “because of the significant U.S.-based DNS expertise and in order to preserve stability.“ (NTIA 1998b). There was no way to link DNS regulation to an international organization or similar intergovernmental body as some commentators had asked for. The strong intention to not let any government influence this central Internet regulation task constantly motivated the U.S. government to hand over DNS authority only to a private institution. However, Washington itself wanted to keep control over the new corporation until its stability allowed to independently continue its work. For this reason, the DOC set up a time frame which expected to keep a close relation between itself and the newly formed corporation until 30 September 2000. Besides that, an exclusive contract was set up in 1998 that gave Washington a certain degree of influence over the new corporation: the Joint Project Agreement (JPO).

Both the JPO (also known as the Memorandum of Understanding between ICANN and DOC) and the location of the corporation (Marina del Rey, California, USA) became serious issues in the following years. Several stakeholders criticized the disproportionate influence of the U.S. government on the Domain Name System. It was frequently mentioned that although Washington publicly declared its intention in the White Paper to render control over the DNS as soon as possible, the institution itself remained on U.S.-American territory and therefore under U.S.-American law. The fact that Washington did not realize or simply ignored the seriousness of this conflict gets reflected in a lapidary statement in the White Paper regarding its critics: "Finally, we note that the new corporation must be headquartered somewhere, and similar objections would inevitably arise if it were incorporated in another location." (idem).

Concerning the constitution of the new corporation the DOC stated that the board of directors had to reflect geographical and stakeholder diversity:

> The Green Paper identified several international membership associations and organizations to designate Board members such as APNIC, ARIN, RIPE, and the Internet Architecture Board. We continue to believe that as use of the Internet expands outside the United States, it is increasingly likely that a properly open and transparent DNS management entity will have board members from around the world. Although we do not set any mandatory minimums for global representation, this policy statement is designed to identify global representativeness as an important priority. (idem).

Another aspect that was highly discussed during the Green Paper process and later adapted in the White Paper was the question of registries[25] and registrars[26]. Both the DOC and the commentators agreed that there should be a competition between registrars. Different than stated before in the Green Paper, the U.S. government decided to hand over the task of creating market criteria for registrars to the new corporation. In the Green Paper the U.S. government still saw the responsibility for this task in its own sphere of control. A similar process was suggested for the question of competition among registries. Concerning this aspect opinions were more diversified.

[25] A registry is an organization responsible for the administration of TLDs. It is directly linked by a contract to ICANN. For every TLD there is one single registry worldwide. In 2010 there were 21 gTLD registries registered with ICANN (USA: 14, Ireland: 2, Switzerland: 2, Hong Kong, Spain, UK: each 1). Besides these registries for gTLDs there are national registries that administrate ccTLDs like .br. In Brazil the national registry is called Comitê Gestor da Internet no Brasil (CGI.br).

[26] A registrar is an organization (or company) providing Internet users with TLDs, usually on a commercial basis. It is a service providers that offers different kinds of IT products like webspace, domains, email etc.

While the U.S. government showed itself in favor of a competition also among registries, a notable number of other actors spoke out for a noncompetitive environment for registries. The White Paper made clear that this question also had to be responded by the corporation to be founded. The same decision was taken regarding the creation of new TLDs. In the White Paper Washington revised its former decision to create a number of new domains on its own. Instead, it was suggested that also in this case the new organization had to take over responsibility.

A further crucial issue was the question of trademarks. When in 1993 users started to register the first Internet domains, it happened on a first-come, first-served basis (Litman 2000). At that time, electronic commerce was largely unknown and the early .com-domains were registered by the then small company Network Solutions which was contracted by the U.S. National Science Foundation (NSF). After it became more obvious that e-commerce was going to be a promising business, several companies wanted to register domains based on their company's or product's name. In several cases trademark owners had to realize that either a different company with the same name had already registered the domain they were looking for, or that private individuals were owning it. In several cases domain speculators had registered high numbers of company or generic names aiming at reselling them to an interested purchaser.

Based on the experience of several domain trademark issues in the past the U.S. government favored a solution that was supporting the private sector to successfully establish a flourishing e-commerce culture. At the same time the DOC acknowledged that not only trademark owners but also Internet users had to be respected and protected in the process of domain name registration. Also an extensive number of other stakeholders underlined the importance of the trademark problem. Especially the creation of public data bases including domain owner information was supported. Furthermore, the installation of online dispute mechanisms regarding trademark issues was debated, “to provide inexpensive and efficient alternatives to litigation for resolving disputes between trademark owners and domain name registrants“ (NTIA 1998b). Another proposal of the DOC regarding the agreement of domain registrants to cooperate on a legal basis was interpreted especially by non-U.S. stakeholders as an “inappropriate attempt to establish U.S. trademark law as the law of the Internet“ (idem), and was therefore disapproved. To find a solution to this question the U.S. government decided to include the World Intellectual Property Organization (WIPO) as an international stakeholder representative into the trademark dispute process. As John Mathiason put

it:

> The Green Paper only said that trademark disputes should be resolved according to national law, while the White Paper recognized the role of WIPO in the process, which was requested to initiate a balanced and transparent process, including the participation of trademark holders and members of the Internet community who are not trademark holders, to develop uniform dispute resolution procedures on trademark and intellectual property holders. (Mathiason 2009, p. 57).

The WIPO approach later resulted in the Uniform Domain Name Dispute Resolution Policy (Froomkin 2002).

After the publication of the White Paper a debate started during which a broad number of stakeholder groups discussed the circumstances under which the new corporation was going to be created. Different stakeholder coalitions were formed with the objective to develop proposals to structure the new corporation that was soon going to take power over the DNS administration. Following Marcus Franda, participants in the debates were among others the Open Root Server Confederation (ORSC), the Boston Working Group (BWG), the Commercial Internet eXchange (CIX), CORE and the World Internet Alliance (Franda 2001, p. 54). The scenario in which the debates took place was called the International Forum on the White Paper (IFWP). Starting in June 1998 the IFWP organized four central meetings in which the participating stakeholder groups had the possibility to elaborate structural suggestions for the new corporation. Antonova defined the mandate of the forum as “to sponsor a framework of coordinated international meetings, to be held around the world, at which stakeholders would discuss the transition to private sector management of the technical administration of Internet names and numbers.“ (Antonova 2008, p. 158). More than 1000 participants attended the four principal meetings that were held between July and August 1998 in Herndon (USA), Geneva (Switzerland), Singapore (Singapore) and Buenos Aires (Argentina). The final meeting was set up to take place in September at the Berkman Center for Internet and Society (Harvard University) but was canceled shortly before due to the activities of a second coalition that met parallel to the IFWP process. Compared to the bright constitution of the IFWP this second coalition, made up of IANA and ISOC, had a relatively narrow composition and represented mainly the technical community while the IFWP also included stakeholders from other sectors of society (Mueller 2002, p. 177).

On 17 September 1998 IANA (together with NSI) released its "Draft Articles of Incorporation and Bylaws of an Internet Corporation for Assigned Names and Numbers (ICANN)" (Antonova 2008, p. 159).[27] With this document the name of the new corporation was officially published and so was its basic structure. Although the IFWP September meeting got canceled, a group of stakeholders that had participated in the forum process reacted on the IANA publication and met up in Boston to discuss the new proposals. On 19-20 September this group, known as the Boston Working Group (BWG), developed the "Boston Meeting Consensus for Changes to the IANA/NSI Draft By-Laws" (BWG n.d.). The document was then handed not only to the DOC but also to the U.S. President's Office.

The IANA/NSI proposal was later chosen by the DOC to be the decisive document upon which the new corporation (ICANN) was going to be built. In fact, the IANA coalition had at that point already registered ICANN as a corporation based in California and had also chosen an interim board of nine directors. This step caused ample criticism among several stakeholders as it was considered to be a non-transparent process executed by a small number of individuals (including Jon Postel and Joe Sims, a Washington-based antitrust lawyer[28]) without consulting the majority of the Internet stakeholder groups that had actively participated in the ICANN preparation process during the past months. "From the moment of its formation (...) ICANN faced obstacles and opposition. The secret selection of the initial board, combined with (depending who you asked) the collapse of, sabotage of, or end-run, around popular alternatives created hard feelings." (Froomkin 2000, p. 82). The decision to dictate ICANN's interim board of directors can be seen as another step towards the difficult stand that ICANN had within the Internet community since the beginning of its existence.

[27] The final version of this document is available at: http://www.icann.org/en/general/articles.htm.

[28] Joe Sims was later responsible for signing the Joint Project Agreement between ICANN and DOC in November 1998.

3.3.3 Constitution of ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) was officially founded on 30 September 1998 as a non-profit private corporation.[29] Since then it is located in Marina del Rey in the U.S. state of California. Following Mathiason, California was chosen as a location "because its laws for not-for-profits were fairly flexible" (Mathiason 2009, p. 58).

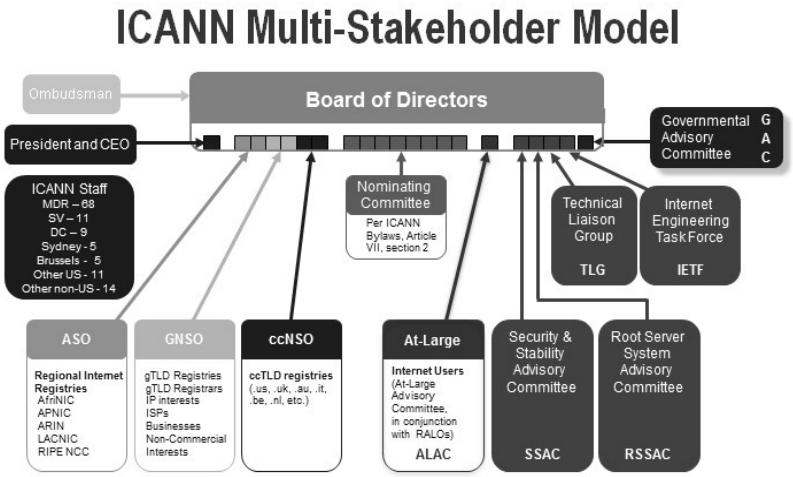
ICANN declares its mission "to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems." (ICANN Bylaws). It furthermore presents in its bylaws the following three main fields of activities:

- to coordinate the allocation and assignment of the three sets of unique identifiers for the Internet (domain names/DNS; Internet protocol/IP and autonomous system numbers; protocol port and parameter numbers),
- to coordinate the operation and evolution of the DNS root name server system,
- to coordinate policy development reasonably and appropriately related to these technical functions.

Despite (or maybe because of) the difficulties and disputes among several actors during the foundation process of ICANN, including the Green Paper and the White Paper process, ICANN tried to create a multi-stakeholder environment in which a large number of stakeholder groups could participate. In the year 2000 it initiated global online elections to let Internet users participate in the constitution of its board of directors (a decision that stands in contrast to the non-transparent constitution of the first interim board that was set up in 1998). For this purpose the world was divided into five regions being Asia-Pacific, Europe, Africa, North America and Latin America (sic) (Pal; Teplova 2004, p. 51). The public interest in the elections was relatively small. About 34.000 out of more than 300 million Internet users worldwide participated in the voting process.

[29] The official foundation document is available at: http://www.icann.org/en/financials/tax/us/appendix-1a.htm

Figure 2: ICANN Structure



Source: http://www.icann.org

ICANN is made up of a complex structure of committees, working groups and task forces. Figure 2 shows the latest constellation of the corporation (2011) and its main bodies that constantly remained over the years. Since its foundation in 1998 a large number of groups and entities have been part of ICANN's structure for a short period of time like the Membership Advisory Committee (1998-1999), the Internationalized Domain Names Committee (2000-2002), the Board and GAC Working Group (2005) or the President's IANA Consultation Committee (2005-2008). Although the constitution of ICANN's organizational structure is of international character there is one major aspect that constantly remained as a heritage of the Internet's geographical origin, which is a close connection to the U.S. government. “The U.S. Department of Commerce (DOC) retained ultimate control of the root, leaving ICANN policy decisions subject to a potential veto. Despite the much-publicized privatization, the United States never completely ceded its hold over the Internet.“ (Klein 2002, p. 201). A similar standpoint was taken by policy analysts of the Internet Governance Project (IGP), a research entity located at the School of Information Studies at Syracuse University (USA). Following an IGP policy paper published in 2005, “political oversight of ICANN exists, but is unilateral: a single government (the US) actively supervises ICANN.“ (Mueller 2005, p. 3).

To prove this argument, the author referred to three specific contracts between the U.S. government and the crucial Internet governance actors VeriSign, IANA and ICANN. These contracts guarantee Washington an important influence on certain aspects of the Internet that are

administrated by the three entities mentioned and will be presented in the following paragraphs.

An early agreement between the DOC and NSI already existed since Network Solutions started administrating the root server A in the early 1990s. In 1991 the company was subcontracted by the Governance Services Inc. (GSI) and later in 1993 took over the registry service from the National Science Foundation (NSF). Since then, Washington was eager to maintain its influence over NSI. In January 1993 the Cooperative Agreement between NSI and the U.S. government (represented by NSF) was set up to assign Network Solutions to provide registration services (article 3). Amendment 11 of the contract also confirmed NSI's control over the root server A.[30] Besides that, the amendment clearly stated that any changes made to the root zone needed an explicit authorization of the U.S. government:

> While NSI continues to operate the primary root server, it shall request written direction from an authorized USG [United States Government] official before making or rejecting any modifications, additions or deletions to the root zone file. Such direction will be provided within ten (10) working days and it may instruct NSI to process any such changes directed by NewCo [ICANN] when submitted to NSI in conformity with written procedures established by NewCo and recognized by the USG. (ICANN 1998a).

When ICANN was founded in 1998 new agreements were arranged between the DOC, NSI and ICANN, like the ICANN-NSI Registry Agreement of November 1999 (ICANN 1999) including regulations for registry services offered by NSI and the respective obligations by ICANN in this context.[31] Regarding Washington's continuing influence in the political oversight of crucial Internet resources and especially referring to the cooperative agreement between NSI/VeriSign and the NSF (which was later replaced by the Department of Commerce) Milton Mueller stated: “The agreement is important for two reasons: 1) it was the instrument by which the U.S. government obtained and continues to exercise its authority to control the root; and 2) it compelled VeriSign to conform to the ICANN regime’s regulations on registries and registrars.“ (Mueller 2005, p. 5).

In February 2000 the *Contract Between ICANN and the United States Government for Performance of the IANA Function* came into force[32] (ICANN 2000). Before the foundation of

[30] The cooperative agreement and its amendments can be accessed at: http://www.icann.org/en/nsi/
[31] Agreements between the DOC, ICANN and NSI can be found at: http://www.icann.org/en/nsi/nsi-agreements.htm
[32] Another preceding agreement had already regulated the transition of IANA from USC to ICANN in December

ICANN, the Internet Assigned Numbers Authority (IANA) was located at the University of Southern California (USC) and was administrated by Jon Postel. The institutionalization of IANA within ICANN was an important step to create a stable environment in which the Internet could develop. During the 1990s the character of the Internet had changed from a pure user network which for a good part was run and administrated by individuals to a more and more commercially usable medium. The institutionalization of central entities like IANA was therefore a logical step. "The new ICANN corporation replaced Jon Postel as the policy authority over the root. ICANN solved the problem of stability: A person was replaced by an institution, so that the IANA could function independently of any one individual."[33] (Klein 2002, p. 201). However, the transition of IANA to ICANN also kept this crucial Internet resource under control of the DOC.

Though, the most disputed contract among the above mentioned was the Memorandum of Understanding (MoU) also known as the Joint Project Agreement (JPA) between ICANN and the DOC. The JPA entered into force in November 1998, a few weeks after the official foundation of ICANN.[34] Its general aim was to enable the DOC to actively attend the privatization process of the DNS. One important aspect in this regard was that the DOC could decide *when* the privatization process was complete (meaning at which point of time the U.S. government would give up or reduce its influence over ICANN). The main objectives of the agreement were stated as following:

> Before making a transition to private sector DNS management, the DOC requires assurances that the private sector has the capability and resources to assume the important responsibilities related to the technical management of the DNS. To secure these assurances, the Parties will collaborate on this DNS Project (DNS Project). In the DNS Project, the Parties will jointly design, develop, and test the mechanisms, methods, and procedures that should be in place and the steps necessary to transition management responsibility for DNS functions now performed by, or on behalf of, the U.S. Government to a private-sector not-for-profit entity. Once testing is successfully completed, it is contemplated that management of the DNS will be transitioned to the mechanisms, methods, and procedures designed and developed in the DNS Project. (ICANN 1998b).

1998: http://www.icann.org/en/general/usc-icann-transition-agreement.htm.

[33] Jon Postel passed away in October 1998, few days after the foundation of ICANN. His outstanding contributions to the development of the Internet are commemorated by both IANA and ICANN who until the present day have links to a Jon-Postel-Memory website included in their own web presence.

[34] The agreement was signed by Joe Sims as a representative of ICANN. A few weeks earlier Sims had announced together with Jon Postel and others ICANN's interim board of directors.

The JPA furthermore defined the DNS management functions that had to be dominated by ICANN before the privatization process would be declared complete. The most important of these functions (based on the specifications of the White Paper) were: 1) the establishment of policy for and direction of the allocation of IP number blocks, 2) the oversight of the operation of the authoritative root server system, 3) the oversight of the policy for determining the circumstances under which new TLDs would be added to the root system, and 4) the coordination of the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet (idem). The time frame defined by the JPA to achieve these goals was until 30 September 2000. However, the JPA was renewed in the year 2000 and several times after that which caused suspicion in the international Internet community that the U.S. government was not willing to give up its privileged position. In 2005 Milton Mueller came to the conclusion that the content of the JPA reflected U.S. policy priorities:

> At present, the MoU's content reflects U.S. policy priorities. It follows the U.S. policy position on new top level domains, privacy in Whois, competition policy, and relations with country code TLD managers. With one-year or three-year renewal periods since 1998, DOC keeps ICANN on a short leash. (Mueller 2005, p. 3f).

Five years later he confirmed his standpoint stating: "The JPA provided a list of policy-making tasks that ICANN is supposed to perform. The specific priorities and milestones in those documents clearly reflected the interests of the U.S. government." (Mueller 2010, p. 63).

When Barack Obama was elected President of the United States in 2008 the debate within the Internet community concerning the JPA received new incentives. Obama's election campaign did not only have a general focus on "change" in several sectors of the U.S.-American society. It also included a strong ambition to leave behind the aggressive unilateral direction that the previous government under President Bush had followed for the foregoing legislative periods. Besides that, Obama's campaign was supported by a strong online campaign including the latest web 2.0 applications which suggested a certain affinity and progressive attitude regarding information technologies (Miller 2008; Kiss 2008). The political scenario favored an end of the JPA that was going to expire on 30 September 2009. In its annual report of 2008 also ICANN itself expressed the desire to be released from political oversight by the DOC:

> The Joint Project Agreement (JPA) between the United States Government and ICANN has as its purpose the transition of the Internet Domain Name System (DNS) to private sector multi-stakeholder leadership. (...)
>
> The Board of ICANN believes the JPA has helped ICANN become a stable organization and that ICANN is meeting its responsibilities. Concluding the JPA in September 2009 is the next logical step in transition of the DNS to private sector management. (ICANN 2008, p. 37)

Within the Internet community it was widely agreed that the DOC needed to end the contract with ICANN. However, there were different opinions about when the final step had to be taken. During the mid-term review process of the JPA in 2008 the International Chamber of Commerce declared that to strengthen the organization for the future a serious discussion about the transition had to start immediately to develop a fully independent organization (ICC 2008). Others like the Center for Democracy and Technology suggested that a complete independence of ICANN remained the ultimate goal but they did not see the time had come to already end the JPA (CDT 2008). The Internet Governance Project at Syracuse University favored an end of the JPA in 2009 but suggested to replace it with “new forms of oversight rooted in the global Internet community“ (IGP 2008). The reason for this was the awareness that ICANN still lacked the ability to independently fulfill its tasks, combined with the wish to reduce or if possible to end the instrumentalization of ICANN as a U.S. policy tool.

One week before the JPA was going to end on 30 September 2009, The Economist explained that “a new accord is planned to come into effect, whereby America will pass some of its authority over ICANN to the 'internet community' of businesses, individual users and other governments.“ (The Economist 2009). The new agreement called Affirmation of Commitments (AoC) responded “to growing international pressure for the U.S. to abandon the control over ICANN that other nations feared gave the U.S. a dominant role over the DNS.“ (Froomkin 2011, p. 189). It gave ICANN more independence than it had under the JPA regime. With the AoC ICANN was not longer obligated to report simply to the U.S. government but to an international committee. However, although this step was welcomed by many JPA critics, it did not overcome another problem which was the lack of regulations based on which it was possible to judge ICANN's performance (Mueller 2009). Besides that, another crucial issue was the remaining contract between the DOC and IANA which gave Washington continuing control over the DNS.

3.4 The UN Process from WSIS to IGF

The international discussion about Internet governance happens to a big part around the Internet Governance Forum (IGF) which was established in 2005 (and took place for the first time in 2006) as a result of the World Summit on the Information Society (WSIS). The following paragraphs are going to focus on the WSIS process which resulted in the IGF whose first mandate ended in 2010.

The WSIS was organized by the UN in the beginning of the new century. It took place in two phases in 2003 (Geneva) and 2005 (Tunis). During the WSIS process a number of official papers and declarations was published like the Geneva Plan of Action, the Geneva Declaration of Principles and the Tunis Agenda for the Information Society. The Plan of Action already stressed the fact that the WSIS process was conducted by a multi-stakeholder environment made up of representatives from governments, the private sector, civil society and international and regional institutions. In *The New Global Politics of Internet Governance* Milton Mueller expressed that these constellations also pointed out a different approach to global governance itself:

> At the summit there was a clash between two models of global governance, a traditional one based on agreements among sovereign, territorial states, and a new transnational order based on private contracts among non-state actors – but dependent on the global hegemony of a single state (the U.S.) for its implementation. (Mueller 2007, p. 217)

And Wolfgang Kleinwächter expressed:

> While one group argued that the Internet should be globally governed by an intergovernmental organisation, others pointed to the fact that the Internet emerged bottom-up in the shadow of governmental regulation and is rather successfully self-organised by non-governmental entities representing the developers, providers and users of Internet services themselves. (Kleinwächter 2007, p. 13)

The choice of topics discussed at the WSIS shows that technical regulation was not the main aspect of this meeting. Development issues were much more important to the participants like the bridging of the digital divide. The OECD defines the digital divide as

> the gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard both to their opportunities to access information and communication technologies (ICTs) and to their use of the Internet for a wide variety of activities. (OECD 2001, p. 5)

It can be seen as a superordinate concept under which different actors with a focus on development politics follow various approaches from improving education and infrastructure to assuring health care or disaster prevention. Some of the goals pointed out in the Plan of Action were therefore similar to the Millennium Development Goals (MDG) like the connection of villages, universities, schools, public libraries, hospitals and governmental departments with ICT until the year 2015. Another emphasis was the improvement of (among others) e-government, e-business, e-health and e-learning with a special focus on remote areas.

As discussions during the first phase of the WSIS were mainly concentrated on development issues the question of Internet governance was left behind until the formation of the Working Group on Internet Governance (WGIG) by the UN Secretary-General Kofi Annan. WGIG's goals were to

> i) develop a working definition of Internet governance,
>
> ii) identify the public policy issues that are relevant to Internet governance,
>
> iii) develop a common understanding of the respective roles and responsibilities of governments, existing intergovernmental and international organizations and other forums as well as the private sector and civil society from both developing and developed countries,
>
> iv) prepare a report on the results of this activity to be presented for consideration and appropriate action for the second phase of WSIS in Tunis in 2005 (WSIS 2003b, p. 6ff).

The results of these tasks have an important impact on the whole Internet governance process as it is happening today. The definition of Internet governance as published in the WGIG report in June 2005 is:

> Internet governance is the development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet. (WGIG 2005b, p. 4)

This definition is multi-stakeholder oriented and shows a close connection to Stephen Krasner's regime definition (Krasner 1984). Furthermore the WGIG also established four key public policy areas which demonstrated its understanding of Internet governance as being more than a question of mainly technical regulation like it is done by ICANN:

> a) Issues relating to infrastructure and the management of critical Internet resources, including administration of the domain name system and Internet protocol addresses (IP addresses), administration of the root server system, technical standards, peering and interconnection, telecommunications infrastructure, including innovative and convergent technologies, as well as multilingualisation. These issues are matters of direct relevance to Internet governance and fall within the ambit of existing organizations with responsibility for these matters;
>
> b) Issues relating to the use of the Internet, including spam, network security and cybercrime. While these issues are directly related to Internet governance, the nature of global cooperation required is not well defined;
>
> c) Issues that are relevant to the Internet but have an impact much wider than the Internet and for which existing organizations are responsible, such as intellectual property rights (IPRs) or international trade. The WGIG started examining the extent to which these matters are being handled consistent with the Declaration of Principles;
>
> d) Issues relating to the developmental aspects of Internet governance, in particular capacity-building in developing countries. (WGIG 2005b, p. 5).

Besides that, the WGIG spoke out for establishing a discussion forum to address Internet governance issues, especially as existing organizations like the OECD which are involved in Internet governance discussions are not open for a big number of developing countries[35]. Based on the WGIG report Internet governance became a more important topic during the second phase of the WSIS in Tunis (2005). During this phase the focus was put on the implementation of principles developed in Geneva.

The most important output of the Tunis meeting was the Tunis Agenda for the Information Society which was published at the end of the meeting on 18 November 2005. It is also considered

[35] The expression “developing countries“ is a highly difficult term as usually a large number of countries are integrated into the same theoretical concept although they have little in common. For this and several other reasons the term merits a critical discussion which however will not be part of this thesis.

to be the constitutional document of the Internet Governance Forum (IGF) a multi-stakeholder discussion forum on Internet governance. The three central topics of the Tunis Agenda were 1) financial mechanisms for meeting the challenges of ICT for development, 2) Internet governance and 3) implementation and follow up.

The first topic (financial mechanisms) was related to the main objectives of development and inclusion already stressed in the Geneva Plan of Action. A Task Force on Financial Mechanisms (TFFM) was established to report on existing and potential possibilities to finance what is called ICT for development (ICT4D). The Tunis Agenda stressed the problematic of the digital divide between industrialized and developing countries. Sustainable investments in ICT infrastructure and services as well as capacity building, transfer of technology and technological cooperation between northern and southern countries were mentioned to be important measures to change the status quo. As investments in the past were mainly done by the public sector it was underlined that also private companies have an important role in the ICT4D process. One example were investments in infrastructure, especially in remote areas. A crucial precondition for private sector engagement is the implementation of policies and regulations to make investments more attractive. In this context the Tunis Agenda pointed out that market forces alone could not solve the problem and therefore international cooperation was important and so was the inclusion of ICT in national development strategies. But not only the national level, also the global level was addressed, especially the necessity of the reduction of international Internet costs to let national providers offer lower prices to end customers. As an interesting and innovative way to finance ICT4D the Tunis Agenda mentioned the Digital Solidarity Fund (DSF) which was established in Geneva and was open to any interested stakeholder.

The second topic of the Tunis Agenda concentrated on Internet governance. It was stressed that the Internet must be seen as a global facility and within the debate about the Information Society Internet governance should play a central role. The importance of a multi-stakeholder environment consisting of governments, the private sector, civil society, intergovernmental and international organizations was confirmed. The before mentioned definition of Internet governance, developed by the WGIG, was accepted and the Tunis Agenda also pointed out that not only technical questions were part of the Internet governance discussion but also public policy issues. By doing so it became clear that not just IP numbers and related aspects dealt with by ICANN, but

several other aspects and topics were also going to be part of the new discussion process on Internet governance. Some of them mentioned were multilingualism, spam, e-business, cybercrime, freedom of expression, privacy, cybersecurity, critical Internet resources, affordability, reliability and quality of service. To distinguish tasks and duties of the different stakeholders the Tunis Agenda already categorized some of the aspects. Policy authority was therefore said to be the sovereign right of states. The private sector was mentioned in relation to development of the Internet in technical and economical fields while civil society was declared responsible for the community level. Intergovernmental and international organizations were said to act mainly as facilitators in the coordination of public policy issues and to set technical standards. The UN Secretary-General was asked to set up a multi-stakeholder policy forum to address these topics. This was to be called the Internet Governance Forum whose mandate until 2010 was defined as to

> discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet...The Internet Governance Forum, in its working and function, will be multilateral, multi-stakeholder, democratic and transparent. (WSIS 2005, p. 11).

Between 2006 and 2010 the IGF happened once a year in Greece (2006), Brazil (2007), India (2008), Egypt (2009) and Lithuania (2010). Each meeting offered a variety of presentations and workshops prepared by members of different stakeholder groups, targeting relevant topics like the future of ICANN, the implementation of technical standards, Internet access in remote areas, or human rights, privacy and freedom of speech on the Internet. Two topics of growing relevance for the Internet governance debate will be discussed in chapter four and five being cybercrime and Internet filtering.

Stakeholder relations within the IGF process can be divided into two principal categories: 1) groups of interest and 2) sector groups. Groups of interest are made up of informal trans-sector coalitions which agree on certain issues. There are four major areas which dominated Internet governance politics during the first mandate of the IGF and which will play a central role for the second mandate as well: intellectual property protection, cybersecurity, content regulation and critical Internet resources (Mueller 2010, p. 127ff). Within these areas of interest stakeholders cooperate independently of their respective sector. While this first category tells about the dynamic character of the multi-stakeholder approach, the second category also shows the conflict lines

between sector groups. In this context it can be stated that the IGF process is divided into supporters of the multi-stakeholder model (civil society, business sector, technical community and a number of governments) and its opponents (other governments).

Although there have been other multi-stakeholder meetings or forums in the past (e.g. at the UN Commission on Sustainable Development or at the International Council for Local Environmental Initiatives) the IGF can be seen as a role model for this form of organizing debates and meetings on the international political level. The importance of the inclusion of several different interest groups became a frequent concern for all Internet governance meetings (with a few exceptions like the French "eG8 Forum"). After two years of the first IGF mandate representatives of the public sector, civil society and the private sector underlined the importance of the multi-stakeholder scenario to create a stable and developing Internet. In an ebook published by Avri Doria, Wolfgang Kleinwächter and the IGF Secretariat in 2008, Maud de Boer-Buquicchio of the Council of Europe underlined that the multi-stakeholder approach of the IGF also had a crucial effect on the organizational structure of inner-European meetings on Internet governance (Doria; Kleinwächter 2008, p. 22). Besides that, she made clear that this relatively new approach applied by the IGF had a constructive influence on communication in other diplomatic fields:

> From the perspective of an inter-governmental organisation (IGO), the IGF is helping the Council of Europe to break new ground in the way in which governments communicate with other stakeholders, in particular the private sector and civil society. In fact, this is the only way in which solutions to the challenges of the Internet can be found, especially considering the predominance of the private sector to advance the Internet via the delivery of applications and services and of the users to use them. The role of the IGF as a model for communication between governments and other stakeholders is increasingly enabling IGO's, such as the Council of Europe, to foster multi-stakeholder dialogue in intergovernmental settings. (idem, p. 23).

Similar to Maud de Boer-Buquicchio also Catherine Trautmann (Member of the European Parliament) expressed the idea that the IGF's multi-stakeholder model could become a role model for future governance processes. Following Trautmann "the IGF is set to be not only a multistakeholder process, but possibly the one to provide new patterns for open and transparent fora on many other subjects." (idem, p. 24). As a civil society representative also Lynn St. Amour of the Internet Society (ISOC) stressed the importance of the multi-stakeholder approach which following her analysis became part of the "Internet Model", a model relying on "collaboration and processes

that are local, bottom-up, and accessible to individuals around the world, whether they are from research, business, civil society, academia, or governments. “ (idem, p. 27). Similar support for the multi-stakeholder model was also articulated by Naoyuki Akikusa, Chairman of the Global Information Infrastructure Commission (GIIC) and therefore representative of the private sector (idem, p. 34).

However, it needs to be considered that especially written contributions developed during the IGF process tend to support the multi-stakeholder approach while critics of this governance model rarely express their point of view concerning the IGF governance model in a written form. This becomes clear especially by taking a closer look at both the academic literature and non-academic reports published since 2006. Publications concentrating on the global Internet governance process and in this context mentioning multi-stakeholderism are also favoring this approach (among others: Antonova 2008; Mathiason 2009; Mueller 2010). This can be explained with the fact that the global debate on Internet governance happens within a truly institutionalist framework while for example a merely realist discourse does not exist at the time, except for a number of individual contributions which however stand mostly for themselves and hardly or do not at all refer to each other. One of the few examples of this realist approach is Goldsmith and Wu's “Who controls the Internet?“ (2006) which focuses mainly on national governments' interests (mostly from a U.S.-perspective) and only mentions the global WSIS/IGF process on one of over 180 pages. Besides that, the authors ignore the multi-stakeholder approach and the central idea of including private sector and civil society actors into the debates. They simply refer to the IGF as a forum “in which governments could debate and make recommendations about Internet policy issues...“ (Goldsmith; Wu 2006, p. 171).

This formulation by Goldsmith and Wu in deed hits the point how a considerable number of national governments preferred the IGF process to happen. Although in most (if not all) publications on the IGF the multi-stakeholder approach is celebrated as an outstanding and necessary concept, its critics have gained ground towards the end of the first mandate. Already during the WSIS process and also in the beginning of the first IGF years several actors supported the multi-stakeholder concept for different reasons. Especially for civil society this new approach was of crucial importance to enter the whole process and not let national governments become the only actors. Also for the technical community the diversification of contributors to the debates was

a way out of the dilemma of letting governments alone decide over the future of the Internet. Following Wolfgang Kleinwächter also the private sector accepted the model after being skeptical in the beginning (Kleinwächter 2011).

The problematic actors within this scenario remain mostly national governments whose representatives tend to speak out in favor of the pluralistic approach but in fact prefer a pure intergovernmental process. This tendency was confirmed during interviews with Drake, Mueller and Kleinwächter who as members of the academic community are involved in Internet governance issues, the WSIS and the IGF process for many years. Therefore governments of highly industrialized and also of several less industrialized countries (developing countries) but also the business community want to reduce the IGF to an annual conference (Drake 2011) while civil society actors are willing to go beyond that by trying to develop new decision-making processes also based on the multi-stakeholder model.

Mueller categorizes supporters of the multi-stakeholder model into strong and weak ones, whereas strong supporters (e.g. civil society) try to improve the IGF process “to make it more thoroughly multi-stakeholder and more influential on policy“ (Mueller 2011). Following his analysis the group of weak supporters (which he also calls “opportunistic“) include the U.S. (under President Obama) and European governments which “wanted to keep the IGF more of an irrelevant talk shop“ (Mueller 2011). In this context a closer look at Maud de Boer-Buquicchio's statement (see above in this chapter) shows that the Council of Europe (as an example for a weak supporter from the public sector) is accepting the multi-stakeholder approach as an innovative form of dialogue rather than a way to reform decision-making processes by including non-governmental actors. This observation goes in line with Europe's traditional understanding of policy development (in this context both, individual European governments and also the European Union can be mentioned): while an effective multi-stakeholder process depends on a transparent bottom-up policy development processes, Europe's understanding of multi-stakeholder participation is limited to dialogues while final policy development processes are still dominated by the classical top-down model (Kleinwächter 2011). On the other hand a certain stagnation concerning progressive innovations of the multi-stakeholder model needs to be considered, putting strong supporters of the multi-stakeholder model into a disadvantageous position. At the end of the IGF's first mandate in 2010 there is a lack of orientation among supporters of the multi-stakeholder approach while its

opponents know they are willing to enter the path of intergovernmental negotiations.

At the same time Kleinwächter mentions another problem within the public sector which reflects those actors that do not fall into Mueller's category of weak supporters but are (more or less) openly opposing the multi-stakeholder model. Especially non-democratic governments (Kleinwächter mentioned China but others can be included into this group as well) are not pleased with the fact that civil society groups which might not be allowed to speak out in their home country gain a (probably uncomfortable) voice during international meetings. Besides that, also critical questions from international civil society actors bring certain governmental representatives in an unpleasant situation. During the IGF 2007 in Rio de Janeiro the author participated in a workshop where within a debate members of international civil society groups confronted Russian governmental representatives with massive cyber attacks on Estonian infrastructure that had happened before in the same year (at that time the Russian government was suspected of being to a certain extent responsible for the attacks). Following Moscow's official line the public sector representative rejected the Kremlin's involvement in a harsh way that prevented a further debate on the issue and at the same time showed civil society actors their unwillingness to debate critical topics. In 2009 another incident demonstrated this partly complicated relation between civil society/the academic sector and the public sector of mostly non-democratic states. In that year during the IGF in Sharm El Sheikh (Egypt) the Chinese government delegation successfully protested against the presentation of *Access Controlled*, a then new MIT Press publication on Internet filtering analyzing filtering processes in China and several other countries. As a result of the Chinese objections the presenters had to take down the publication's advertisement banner (referring to Chinese Internet filtering practices) which left them and other members of the third sector in a questionable situation regarding equality of all stakeholder groups within this UN process.

Chapter Four: Cybercrime

Cybercrime is a phenomenon that takes place within the broader context of cybersecurity which Mueller defined as one of the main areas of Internet governance (Mueller 2010, p. 5). To understand the problem of virtual crimes it is therefore necessary to understand the bigger context of cybersecurity. Cybersecurity as a concepts has three different categories being cybercrime, cyberterrorism and cyberwarfare.

In the ordinary user context of online security, cybersecurity could be a simple form of corporate network protection or private protection against spam or other malware distributed on the Internet. It could also mean protecting family members (for example children) from accessing unwanted web content. Furthermore it means protection from ordinary crime or fraud occurring on the Internet like phishing, identity theft, credit card fraud and others (McQuade III, 2006, p. 63ff). These types of activities are also categorized as cybercrime. Cybercrime itself does not have a purely economic side but can also have a political dimension. Examples for political cybercrimes are hate speech and cyberterrorist activities. Besides that, politically motivated cybercrimes can happen in a broader context that include espionage or international conflicts which will be discussed later in this chapter. Hate speech usually refers to racist, anti-semitic or anti-ziganistic content that is clearly of political nature but is also treated as a cybercrime when it happens online.

Cyberterrorism (or cyberterror) is a more complex concept. It could be treated as a cybercrime in certain cases like the distribution of information to produce explosive devices. Nevertheless as the case of three young men in the UK shows, governments are tending to recognize such activities as acts of terrorism rather than simple cybercrimes (Stevens, 2008).

Terrorist groups are using the Internet for a wide spectrum of activities ranging from spreading information and propaganda, over networking and recruiting, until mobilization and fundraising (Weimann 2006, p. 111ff). Mehan defines cyberterror as “the politically-motivated use of computers by terrorist groups, sub-nationals, or clandestine agents as weapons or as targets intended to result in violence, influence an audience, or affect national policies.“ (Mehan 2008, p. 33). Her definition is based on two other definitions given by 1) the 22 U.S. Code, section 2656, and 2) the U.S. National Infrastructure Protection Division (NIPD). The first one mentioned

concentrates on terrorism in general and says that it can be described as “premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience.“ (idem, p. 32). Following the NIPD “cyberterrorism is a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies.“ (idem, p. 32). A crucial point in Mehan's definition is the clarification that computers can be used “as weapons or as targets“. This becomes clear when referring to Kerr's contribution to the discussion on cyberterror in which she mentioned that out of 109 definitions of cyberterror four mentioned all of the three main aspects 1) use of violence, 2) political objectives, and 3) the purpose of spreading fear within the population (Kerr 2004). Nevertheless two of those definitions refer to computers as being targets, the other two as being means of an attack. Mehan assembled these two different approaches and created a more complete definition of cyberterror.

The third category of cybersecurity is cyberwarfare (or cyberwar). Cyberwarfare can be seen as a sub-category of information warfare, a term introduced by the U.S. military in the 1980s which includes the domination of all possible means of information and communication (including psychological operations) to use them against the opponents. Different from information warfare, cyberwarfare is limited to the usage of computer networks to harm a country's critical infrastructure. By definition of the European Commission, critical infrastructure stands for

> those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical Infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services. (Commission of the European Communities 2004, p. 3).

Mehan distinguishes four different kinds of cyberwar:

> (…) Class I cyberwar is concerned with the protection of personal information (…). Class II cyberwar concerns itself with industrial and economic espionage (…). Class III cyberwar is officially about global war and terrorism (…). Finally, Class IV cyberwar is the use of all the techniques of Classes I-III in combination with military activities in an effort to obtain a battlefield advantage or a force multiplier. (Mehan 2008, p.

28).

Early cyberwar attacks go back to the 1980s when the U.S. used hacking methods to infiltrate computer networks of the Soviet Union, mainly with the intention of espionage. With the further development of IT networks in the 1990s the Kosovo war in 1999 saw the first big application of cyberwar measures. While the U.S. used different methods to manipulate Serbian weapon and communication systems (Arkin 1999; Dunn 2001), also the Serbian and Albanian side used IT to support their own strategies. In most cases this involved spreading information and propaganda accusing the other side of war crimes and cruel activities but also to connect with supporters or diaspora in other countries. Furthermore NATO and U.S. servers were attacked. When in May 1999 the U.S. bombed the Chinese embassy in Belgrade, a wave of cyber attacks from China hit U.S. and NATO infrastructure (Messmer 1999) many of them being denial-of-service (DoS) attacks conducted by private citizens from their home computers in what Timothy Thomas of the U.S. Foreign Military Studies Office called a "take-home-battle" (Thomas 2000).

Besides simple hacking activities to access information on foreign computers, spreading malware, or changing website content (website defacement[36]), DoS attacks are one of the most frequently used measures to conduct virtual attacks. The effect of such an attack is the inability to access a network or information on a website. DoS attacks can cause massive data traffic on foreign networks which as a consequence break down temporarily. The better protected the network under attack, the higher the necessary number of attacking computers. While for a simple server a few hundred computers can already cause problems with data processing, government networks or those of bigger companies are more difficult to corrupt. In that case distributed-denial-of-service (DDoS) attacks can be operated as they include a higher number of computers that can be controlled by one single person. Before launching a DDoS attack the aggressor needs to get control over a number of computers which are usually kidnapped online from ordinary users who are unaware of their unwanted participation in the attack. To get access to other computers, malicious codes distributed by spam, fraudulent websites, or other means of capture are connecting private user PCs to a controlling server. An aggressor can also easily get access to a required number of captured computers by simply hiring botnets online.

[36] One example for a massive web defacement campaign are the cyber attacks on Brazilian governmental infrastructure in June 2011 (Oppermann 2011).

Originating from the suffix of “robot“, a botnet consists of several computers under control of a single authority (bot herder) which can command the single units (drones or zombies) of the botnet to simultaneously access a chosen network at a specific point of time. This kind of DDoS attacks based on botnets are common virtual attacks and can be executed by a single person. Botnets are offered for hire to cybercriminals, cyberterrorists or any other form of cyber aggressor. Contact between supplier and renter can be made on several forums on the Internet. The prices differ from 50 U.S. dollars per day for a small botnet up to thousands of dollars for more complex networks. In 2009 huge botnets existed consisting of millions of captured computers (Grant 2009). Generating botnets became a worthwhile business supplying thousands of cyber aggressors who altogether paid several million dollars to botnet providers.

4.1 Historical Roots and Development of Cybercrime

In the first decade of the 21st century cybercrime as a phenomenon as gained growing attention in a number of countries. Especially those who possessed a well developed IT-infrastructure put cybercrime on a top position of their political agenda. While for a long time most of the servers hosting malware were located on the territory of the USA latest developments showed that China is taking over this leading position. Besides those two, also Russia and Brazil play important roles in worldwide cybercrime occurrences. China, Russia and Brazil have a fast growing IT-infrastructure, growing numbers of users and no sufficient cybercrime legislation so far. But not only nations and governments play an important role in the cybercrime context. There is a number of other actors that need to be included to understand the complete picture of cybercrime as will be shown in the following paragraphs.

Although only in the 21st century cybercrime became a major issue, it already existed for decades. To understand the different historical stages of cybercrime it can be classified into three phases: the pre-network phase (1950-1969), the early network phase (1969-1990) and the commercial network phase (since 1990).

The pre-network phase began with the spreading of early computer systems in the 1950s. These mainframe computers had been developed already since the 1930s, but only with the construction of the UNIVAC computer in 1951 the first wave of commercialization of mainframe computers started. Two years later also the first IBM mainframe computer was presented. Mainframe computers where big-sized calculation machines that required an investment of several millions of U.S. dollars. They came to use mainly in bigger companies or government agencies. Due to their size and cost companies hardly had more than one exemplar. At the time of the early mainframes, networking between computers was still unknown. Cybercriminal activities were therefore limited to the machines the users had direct physical access to. Besides this geographical constriction also the number of potential delinquents was very small. The complexity of mainframes required specialized personnel. Those were the only individuals capable of operating computers. Early cases of cybercrime were therefore conducted by employees harming their own employers, usually by conducting fraud or embezzlement (Brenner 2010, p. 10f). It remains unclear how many cases of early cybercrime really happened as usually the responsible employees where the only ones knowing about their illegitimate activities.

The pre-network phase also saw the upcoming of a type of tech-savvy individual that had a crucial role in later development of the Internet for the good as for the bad. In the late 1950s a group of students at the Artificial Intelligence Laboratory of the Massachusetts Institute of Technologies (MIT) started what became known as “hacking“: they manipulated mainframe computers letting them conduct a series of unusual activities. One of the most famous manipulations was the programming of the “cookie monster“ hack. Once a computer was manipulated with a “cookie monster“ hack it would ask the user for a cookie who on his part could end the query by typing “cookie“ into the machine. This program demonstrates the characteristics of original hacks before they became known as objectionable cyber attacks. Early hackers were driven by the motivation to let mainframe computers carry out small-scale operations that did not necessarily have a productive function but also had no malicious intention. They were much more seen as a humorous way to explore computer systems. RFC 1983 describes a hacker as: “A person who delights in having an intimate understanding of the internal workings of a system, computer and computer networks in particular.“ (Malkin 1996). Early hackers at the MIT were in fact influenced by the anti-war movement of the late 1960s. Free access to information was one of their principle objectives (Rosenzweig 1998, p. 1542), a popular demand of pacifist student groups that were aiming at

ending classified military research projects (idem, p. 1541f). Also Steven Levy highlighted the idealist attitude of the early hacker generation. He called it “a philosophy of sharing, openness, decentralization, and getting your hands on machines at any cost to improve the machines and to improve the world.“ (Levy 1994, p. 4).

The idealism of hacker groups got challenged during the early network phase with further advancement of technology, especially the successful connection of individual computers in the late 1960s and the diversification of computer systems. As had been shown before, researchers at the MIT first connected small numbers of computers in different universities and later built bigger networks, including the ARPANET. The possibility to create computer networks also resulted in an increase of hacker activities. Moreover the diversification of technology lead to a diversification of the hacker culture as well. The invention of new operating systems and programming languages over the following years resulted in a classification of hackers. Eric Raymond called it the

> (...) three cultures, overlapping at the edges but organized around very different technologies. The ARPAnet/PDP-10 culture, wedded to LISP and MACRO and TOPS-10 and ITS. The Unix and C crowd with their PDP-11s and VAXen and pokey telephone connections. And an anarchic horde of early microcomputer enthusiasts bent on taking computer power to the people. (Raymond 1999, p. 23).

Another boom in hacker activities happened with the commercialization of personal computers (PC). Companies like Apple, Commodore and IBM presented their first PCs in the late 1970s and early 1980s which attracted thousands of youths to start hacking. Being outside of the classical hacker environments at the universities, a growing number of hackers turned out to become black hat hackers. Black hat and white hat hackers became widespread expressions to clarify whether a hacker's intention was of positive or negative nature. A black hat hacker was also termed as a cracker which was defined in RFC 1983 as “an individual who attempts to access computer systems without authorization. These individuals are often malicious, as opposed to hackers, and have means at their disposal for breaking into a system.“ (Malkin 1996). Different than white hat hackers, whose central objective was to share information with as many people as possible on a non-commercial basis, crackers showed no hesitation to use their abilities to break into proprietary systems, to cause harm by destroying data or to achieve financial gains for themselves. During the 1980s a number of individuals or groups acted in this manner, like the 414-

hacker group from Milwaukee (USA) whose members hacked several networks, among them a bank, a hospital and a nuclear weapons laboratory in the state of New Mexico (Murphy; Elmer-DeWitt; Krance 1983).

When the commercial network phase started in the 1990s, hacking became easier and more common among Internet users. While computer networks had been relatively small in the previous decades, the commercialization of the Internet (due to the development of HTML and the first browsers) resulted in faster growing networks that also included small enterprises and private computers. At that time the necessity of network protection was unknown to most Internet users. This high amount of low or unprotected networks offered not only an easy terrain for cybercriminals but also a training area for a new generation of unexperienced hackers who improved their hacking skills at the expense of average Internet users. The vast increase of potential goals for hackers lead to a professionalization of illegitimate use of networks and a sophistication of cybercrimes including the emergence of malware.

Malware (a portmanteau of “malicious“ and “software“) plays a major role in cybercrime and today consists of a steadily growing number of software types. The first type of malware was the computer virus, a self-reproducing software, developed to infect an unlimited number of computers which is usually spreading over networks. Depending on the intention and the skills of its programmer, a virus can seriously damage computer systems. However, the first known virus (Creeper) was developed as an experiment by Bob Thomas at BBN in 1971 and spread over ARPANET (Chen; Robert 2004, p. 268). It caused no harm but was meant to demonstrate mobility within the network. As it did not damage any files but only replicated itself it can technically be seen rather as a worm than as a virus. Short time after its appearance it was deleted by another program called Reaper.

The idea of self-reproducing software has its origin in the first half of the 20th century when computing was in its early stages and computer networks like ARPANET were still unknown. Chen and Robert (idem) refer to the work of John von Neumann who in 1949 published his research on self-reproducing machines called *Theory of self-reproducing automata*. Furthermore Filiol (2005) points out that von Neumann's work was based on Alan Turing's research from the 1930s who therefore can be considered (together with von Neumann and others) a pioneer in software

(including malware) development:

> A Turing machine ... is the abstract representation of what a computer is and of the programs that may be executed with it. … Only a few years later, the concept of self-reproduction [which was essential for a virus] was considered by John von Neumann and Arthur Burks … starting from the Turing's works and results. (Filiol 2005, p. 7f).

The first viruses and worms that spread outside of a controlled network environment appeared in the beginning of the 1980s. One of the first well known viruses was the Elk Cloner that was developed in 1982 by 15-years old high school student Rich Skrenta in Pittsburgh, USA (Brenner 2010, p. 21). In the following almost three decades, quantity and quality of viruses and other malware grew constantly. At the end of 2009 more than 5,7 million malware programs were found on the Internet (Fossi 2010, p. 47). Today there are several types of malware besides viruses and worms like trojan horses, spyware, backdoors, rootkits and more, each with a different function (McQuade 2006, p. 64f). In the first decade of the 21st century also blended threats (combinations of different malware programs) increased considerably and caused some major problems to the Internet (Higgins 2003, p. 7).

4.2 Stuxnet

There is an undefined number of malicious codes, worms and viruses which were developed by an immense number of programmers worldwide. Although the IT security industry is constantly trying to develop the latest protection for information networks against cyber threats a certain number of malwares became notoriously famous for their destructive success in the past years, e.g. Conficker, Koobface, Zbot or SQL Slammer. Besides those, another piece of code called the Stuxnet worm attracted public attention in 2010. The novelty of Stuxnet was its focus on massive industrial sabotage rather than pure financial gains. Furthermore, a strong political motivation was involved in its development.

Stuxnet was developed on a very different level speaking of professionalism and budget compared to its predecessors. Its complex structure based on different programming languages

indicated that a larger team of professional programmers was working on it for several months which caused expenses of a few million dollars. This assumption supported early theories that Stuxnet was the result of a government-backed project rather than a private hacker initiative.

After being detected by IT security analysts in Belorussia in June 2010 several IT security analysts in the USA and Germany found out that the worm, which at the moment of its discovery had already been around for two years, had not only a notedly complex structure but was also programmed not to manipulate any personal computer (like usual malware does, basically for financial reasons). Instead, it was to focus on Simatic WinCC Step7, a software developed by the German company Siemens to control industrial systems. Also its geographic concentration on Iran distinguished it from former malware. Following Symantec analysts, about 60% of Stuxnet infections were found in that country (Zetter 2011). After analyzing the code it became clear that not espionage but secret manipulation of a specific industrial system was the worm's task. After it recognized the existence of WinCC software, the program would automatically load a number of files into the system where it would hide for two weeks before being activated (idem).

By following the unique ID numbers of the communication components mentioned in the code, Symantec's analysts came to the conclusion that the components Stuxnet was willing to manipulate were frequency converters produced in Finland and Iran which served to define the speed of motors used in specific industrial elements. Once activated, the worm would speed up the motors for a certain time frame before going back to its standard speed which was indicated in the code as 1064 Hz. Following David Albright of the Washington-based Institute for Science and International Security (ISIS) this frequency referred exactly to the centrifuges used in Iran's nuclear enrichment plant Natanz (Albright; Brannan; Walrond 2010). At that time Natanz was a crucial part of the international debate on Teheran's nuclear program (Rudolf; Lohmann 2010, p. 14). Also another aspect supported the theory of Natanz being the target of the attack: Stuxnet was focusing on components organized in groups of 164 units. Also the centrifuges in Natanz were organized in groups of 164 units.

In January 2010 the International Atomic Energy Agency (IAEA) which was controlling Iran's nuclear program, found out that an estimated number of 1000 to 2000 centrifuges had been exchanged in Natanz for unknown reasons in a few months. The regular number of exchanged centrifuges was 800 distributed over the whole year. Later Iran's President Ahmadinejad declared

that different to his previous statements on the issue, a virus had in deed manipulated a number of centrifuges and had caused a delay in the country's nuclear program (Borger; Dehghan 2010).

Although no individual or organization has so far taken responsibility for Stuxnet, the facts underline that it was part of a wider project of industrial sabotage. Especially the necessary budget for development and the sophistication of the code support this argument. Furthermore its focus on a certain industrial environment in a specific region which at that moment was part of a conflict over the potential development of nuclear weapons make clear that elements of cybercrime are also applied in political circumstances by actors which could be but not necessarily are part of an ordinary cybercrime scenario. In the first decade of the 21st century there were more cases of cybercrime which similar to Stuxnet happened within political scenarios but nevertheless are considered cybercrimes. The following chapter is concentrating on this political dimension of cybercrimes.

4.3 Political Dimensions of Cybercrime

With a few exceptions ordinary forms of criminal activities are happening in situations where offender and victim are staying in the same location or at least the same country. This paradigm has changed with the increase of cybercrime. A virtually committed crime can include a number of countries and a number of different legislations. Besides the possibility of the offender being in country A and the victim being in country B there is also the possibility that the infrastructure used to commit the crime (for example a server) is located in country C. This means that law enforcement is extending over three different legislations. Which already in the non-virtual world turns out to be a major challenge (cross-national cooperation of criminal prosecutors) becomes even more complicated when the Internet joins the scene. Not only the difficult tracking of online perpetrators but also the lack of a respective legislation can impede the success of the investigators. Besides that, countries tend to have differing opinions about what can be considered a crime and what cannot. Although this problem already existed long before the Internet was created, the network facilitates cross-national criminal activities by shortening the distance between individuals in different parts of the world.

In the first decade of the 21st century a number of countries was facilitating cybercrime activities by lacking a respective legislation or by simply ignoring the problem. This way, notorious cybercrime havens came into existence, among them were Russia, China (Dixon; Ahmed 2008) and Romania (Boyd 2003) which major cybercrime offenders chose as both their physical and infrastructure locations. In the following years a number of other countries joined the cybercrime scenario. Especially emerging countries like Brazil and India increasingly became victims of cybercriminal activities due to their growing but less protected infrastructure, joining early industrialized countries like Germany, the UK and the USA which had suffered cybercrime activities for many years already (Fossi 2010).

Taking a look at the motivation of cybercriminals one can find mostly economical reasons. The global cybercrime scenario became a constantly growing business with low risks and high revenues. Following a report published by the Council on Foreign Relations in 2010 (in which the author referred to data of the IT security company McAfee), the annual damage to the global economy in 2008 due to cybercrime was about one trillion U.S. dollars (Knake 2010, p. 5). Although this number includes several maintenance costs for the affected companies it also demonstrates the value of data abstracted by the offenders and allows conclusions about the profits made by cybercriminals. In another investigation conducted by the Ponemon Institute researchers observed that all 45 organizations participating in the study had a yearly loss between 1 million and 52 million U.S. dollars (Ponemon Institute 2010, p. 3).

However, there are different profiles of cybercrime delinquents. Besides a large number of so called script kiddies,[37] there are ordinary criminals abstracting credit card numbers, user passwords and more. Besides that in recent years researchers have been analyzing the question if organized crime is happening on the Internet as well. In this context, Choo categorized cybercrime delinquents into three groups: 1) traditional organized criminal groups which try to expand their field of activity on the Internet, 2) organized cybercrime groups operating exclusively on the Internet, and 3) politically or ideologically motivated groups using the Internet for illegitimate activities (Choo 2008). Comparing the first two groups it becomes clear that organized crime in the non-virtual world differs a lot from what Choo categorized as organized cybercriminal groups. While traditional organized crime groups include a large number of individuals and have a certain

[37] Script kiddies are young people, usually teenagers, who access basic hacking instructions or use pre-developed scripts available on the Internet and spend their free time on attacking websites without serious economical interests.

structure, organized cybercrime groups are so far known for their low number of individuals involved. Besides that they can but often do not have a formal structure as their members meet only online. It is even questionable, if organized crime online can be considered a serious threat as most cybercrime activities are easily conducted by individuals. Regarding this question, Marco Gercke of the German Cybercrime Research Institute pointed out in a report for the UN that specific cybercrime activities like identity theft and child pornography do not fall into the category of organized crime (UNODC 2010, p. 207ff).

When it comes to Choo's third category concerning politically or ideologically motivated cybercrimes he distinguished in two sub-categories in which actors use the Internet (or other communication technologies) as a simple means to enable their activities (e.g. spreading hate speech) or in which the Internet itself becomes the crucial technology to conduct a crime like a DDoS attack (Choo 2008, p. 282ff). In fact, this distinction does not refer only to politically motivated cybercrimes but to any form of cybercrime.

In certain cases when the Internet is used as a crucial technology to conduct a cybercrime it is also possible to detect a convergence of ordinary cybercrime and political actions. In these cases politically motivated actors use cybercrime methods for their own ideological objectives. However, these processes do not require that political activists possess an advanced technological know-how. They rather use the infrastructure provided by ordinary cybercriminals. A common way to do so is the provision of botnets for politically motivated DDoS attacks. Political actors hardly have the time or technical knowledge to set up large botnets. For this reason ordinary cybercriminals temporarily rent out botnets in times of political tensions. This phenomenon was extensively noticed during some of the largest and widely observed cyber attacks of the past ten years in which the infrastructure of two post-Soviet states (Estonia and Georgia) suffered serious attacks during political tensions with Russia. Besides that, China is frequently mentioned in relation to cyber attacks on different states in the past ten years in which IT analysts also see an involvement of typical cybercrime instruments like botnets. For this reason there will be a focus on both countries and their involvement in cybercrime or cyber attacks on the following pages.

4.4 Cybercrime and Political Cyber Attacks

The majority of virtual attacks stays unknown from the public. Whenever detected by the attacked, the first priority for the victims is to reduce damage. Especially larger companies but also governmental institutions suffer frequent cyber attacks although they do not necessarily cause serious damage nor do they regularly have a political background. The reasons for not publicly debating all virtual attacks are therefore a question of quantity and (lack of) quality of the attacks, but also to hide vulnerability of the victim. A public or private entity being known for its defectiveness towards virtual attacks (and therefore sensitivity for espionage) would easily loose its reputation which could cost clients, partners, or votes. Cyber attacks that do appear in the media are usually 1) of larger dimension, 2) have a serious economical or political impact, or 3) are published in strategic moments. One example for the first two categories are the attacks on Estonia in 2007 when both the questions of dimension and seriousness came together. Also the cyber attacks during the Caucasus war in August 2008 belong to these categories (see more details on both conflicts later in this chapter).

Examples for virtual attacks that became public in strategic moments are the attacks on German, British, and U.S. government networks publicly announced in August 2007, and the DDoS attacks on U.S. American and South Korean government and business websites in July 2009. In the first example the German magazine Spiegel revealed on 25 August 2007 that cyber attacks on German government institutions like the Ministry of Exterior, the Ministry of Education and Research, the Ministry of Economy and the office of chancellor Angela Merkel had happened with the intention of installing spyware. The actual problem had already been recognized by IT security analysts months before but became a bigger issue at the dawn of Chancellor Merkel's visit to the Chinese government starting on 26 August 2009. In the following week the Spiegel and other newspapers additionally published articles about similar incidents in the U.S. and the UK which also had happened some time before (Spiegel Online 2007a; Sueddeutsche.de 2007b). The intention of these strategically published articles to start a German-Chinese dialogue on the issue was successful. Chancellor Merkel and Premier Wen Jiabao discussed the problem with the result that Wen declared the rejection of the Chinese government to conduct cyber attacks. Contrary to this statement the German Domestic Intelligence Agency (Verfassungsschutz) declared having traced back the attackers to computers of the Chinese Army (Spiegel Online 2007b).

While the case of the German government networks was discovered long before its coverage in the media, the example of the 2009 DDoS attacks on the USA and South Korea did happen at a strategic moment and were immediately published. On the American Independence Day 4 July 2009, 27 U.S. governmental and later also business networks became victims of a DDoS attack which later was expanded on South Korean official and private economy networks. Some of the victims in the U.S. were the Treasure Department, the Secret Service, the Federal Trade Commission, the White House, and the New York stock exchange while in South Korea the Presidential Blue House, the Ministry of Defense and the National Assembly were being attacked. The botnet used to conduct the DDoS attack consisted of 50.000-65.000 computers. The attack can therefore be considered a smaller incident. Nevertheless several systems under attack broke down for up to five days. Further risks like the possible abstraction of information shortly before the attack were mentioned by the Commission on Cybersecurity but could not be proven (Chabrow 2009).

South Korean intelligence analysts suspected foreign governments or pro-foreign government groups without directly mentioning North Korea. U.S. American IT security experts assessed the attack to be little sophisticated judging from the simple character of the scripts used. This would also weaken the theory of the Commission on Cybersecurity about the probability of an act of espionage. What was expressed by the American analysts is that the script referred to China's internal routing system and that it contained data that could be traced back to a Korean-language browser (Markoff; Sang-Hun 2009). Beyond these technical details no individuals or institutions could be made responsible for the incidents.

Besides China, Russia is the second country that is mentioned above average when it comes to cyber attacks. From January to March 2009 different embassies of India, Portugal, Ethiopia, and Azerbaijan have reportedly been under virtual attacks (Constantin 2009a). In the months before, also embassies and consulates of the U.S., Brazil, France, Syria, and the Netherlands suffered cyber attacks (Constantin 2009b). As cyber attackers usually do not leave written messages justifying their course of action it is difficult to analyze the reasons for all virtual attacks which happen and become public. Nevertheless in some cases like the parallel attacks on different websites connected to the Azerbaijanian government in March 2009, it is possible to draw connections to offline

politics. During the week of the attacks, the Russian Foreign Minister Sergei Lavrovis was visiting Azerbaijan while Azerbaijans President Ilham Aliyev left the country to visit Iran. Although this still leaves open the question how this act was interpreted by the cyber attackers who were described by an IT security analyst as members of the Russian cybercrime organization Russian Business Network (RBN), a non-registered company working on an anonymous basis using more than a dozen synonyms in different countries. The RBN can be seen as a crucial non-state actor in cyber attacks worldwide, whose members act as mercenaries for political or private economy interests. More on the RBN's role in politically motivated cyber attacks will be discussed later in this chapter.

Whenever virtual attacks on governmental institutions are discussed the question of responsibility comes up. Although in many and especially in cases of serious damage governmental representatives express suspicions, which are usually based on general political circumstances or on results of IT security analysts, it is almost impossible to prove where cyber attacks come from due to the character of the networks or the fact that botnets are used whose drones do not lead to the location of the real attacker. Furthermore cyber aggressors could use proxy servers to disguise their real location. Also the attack on the U.S. American electricity grid in April 2009 lead to statements by U.S. officials holding China and Russia responsible for infiltrating critical infrastructure on U.S. territory without being able to prove it (Gorman 2009). So far it is unclear in International Law what rights states have to react on virtual attacks. It is undefined if cyber attacks can be categorized as “armed attacks“ which would give states the possibility of self-defense following article 51 of the UN charta. Moreover it is open who they could attack as an act of self-defense. This problem of anonymity of cyber attacks also becomes clear in the following paragraphs which take a closer look at the largest virtual attacks on nation states in the early 21st century.

4.4.1 Russia

Following the International Telecommunication Union, 32,11% of Russia's 140 Million inhabitants were using the Internet in 2008, 21,49% had their own Internet access (ITU Internet Statistics 2008). The country has one of the fastest growing Internet populations in Europe and the bordering regions. Following a research report of the Reuters Institute for the Study of Journalism

at the University of Oxford, Russian users are mostly interested in websites containing sports, music, social activities and other forms of entertainment (Fossato; Lloyd, Verkhofsky 2008, p. 14) plus the steadily growing blogosphere which had about 3,8 million blogs in 2008 (Fossato; Lloyd, Verkhofsky 2008, p. 14). Furthermore the report stated the Russian government under President Medvedev and former President Putin refrained so far from extended Internet regulations which fostered economic development of the ICT market in recent years. Although some exceptions were made for the Federal Security Service FSB, which has the possibility to control Internet communication without knowledge of the Internet Service Providers (ISP).

However, researchers of the OpenNet Initiative see Russia's role in Internet regulation with more critical eyes. In a regional report about the Internet in the Commonwealth of Independent States (CIS) the authors argue that in Russia (and other member states of the CIS) a general tendency “toward greater government regulation of the Internet“ can be observed, “to bring it in line with existing regulations that control the mass media“ (Deibert; Palfrey; Rohozinski; Zittrain 2008, p. 180). The authors also refer to the SORM II regulation which since the year 2000 offers the FSB advanced possibilities to control Internet communication within Russia. SORM II is comparable to a number of laws and regulations passed in the USA after 9/11 like the U.S. Communications Assistance to Law Enforcement Act or parts of the Patriot Act.

The percentage of Russian Internet users who go online for political reasons is quite small. Political activism on the net does partly happen but is also closely watched by national authorities. Nevertheless Russian communication networks have played a crucial role during political crises or conflicts with the nation's neighboring countries. The two major events in this context are the conflicts with Estonia in April 2007 and with Georgia in August 2008. Both countries have a tense relation to Russia due to their history as members of the Soviet Union. The following paragraphs will concentrate on both crises in which cyber attacks happened on the critical infrastructure of both countries.

4.4.1.1 Estonia

As many East European countries also Estonia has a multi-ethnic population, made up mainly of Estonians, Russians, and other smaller minority groups. Early Russian settlements in Estonia go back to the 17th century when a few thousand Russians migrated to the neighboring country escaping religious persecution in Russia. During WWII Estonia was occupied by the Soviet Union (USSR) in 1940 (later by Germany and then again by the USSR) and declared its independence in 1991. During the 5 decades of being part of the Soviet Union, Moscow forced their own population policy on Estonia in the same manner as on other countries within their sphere of power (Rannut 2004). Thousands of Estonians were settled by force to the Russian main territory while thousands of Russians moved to Estonia. By this measures the Russian part of the population of Estonia went up from 8% before the occupation to about 30% until 1991. This percentage went down to around 25% after the independence of the country.

Figure 3: Map of Europe and Russia

Source: Nationalgeographic.com

As Russian was used as an official language for 50 years, many Russians never learned to speak Estonian. With the independence also the Estonian language was reinstalled as the official language of the country, leaving the problem, that about 85% of the Russian minority were not able to speak the new official language, which was 21% of the country's whole population. Since then ethnic minority rights have been a constant challenge for Estonia and relations between Estonians and Russians were tense at certain moments (Lang 2008; Vetik 1993).

One of this moments was the decision of the Estonian government in April 2007 to remove a statue of a Russian soldier from a central place in the capitol Tallinn to move it to a military cemetery outside the city center (Spiegel Online 2007d). The statue had been placed in the center of town by Moscow in 1947 to celebrate the end of WWII. The Estonian population considered it a symbol of occupation. The moment to remove the statue at the end of April was strategically chosen as the Russian-speaking minority used to meet frequently at the statue on 9 May to celebrate the end of WWII.

The decision to relocate the statue caused protests mainly under young Russian-speaking Estonians that turned to riots on 26-27 April during which one person was killed and more than 1000 arrested. In the days after the unrests Russia criticized Estonia for its decision regarding the statue and requested the resignation of the government in Tallinn while anti-Estonian manifestations took place in front of the Estonian embassy in Moscow (Sueddeutsche.de 2007a).

At the same time when the unrests started, cyber attacks were launched on several parts of the Estonian IT infrastructure (Hansen; Nissenbaum 2009, p. 1168f). In the years before, the country had built up a highly sophisticated network environment ranking among the most developed systems worldwide. E-government services were implemented ranging from simple administration services to online elections. At that time, besides governmental services also the banking system and other sectors were based to an above average degree on IT networks. Due to the cyber attacks carried out for about three weeks, large parts of the country's infrastructure suffered breakdowns, including governmental and banking infrastructure, and several online news services. To protect its infrastructure from foreign attacks Estonian Internet Service Providers blocked online queries from outside the national borders. This caused access problems for a great number of companies and private clients to financial resources within the Estonian Hansabank

(Swedbank), one of the biggest financial institutions of the Baltic region. The attacks differed from similar incidents in other countries because of its comprehensive character impacting a whole country instead of individual institutions. Being concerned about the occurences also the European Union condemned the attacks although due to the upcoming EU-Russian summit officials refrained from addressing Moscow for possible responsibility. The NATO sent IT security analysts to Tallinn to investigate. One year after the attacks the alliance opened up its Cooperative Cyber Defence Centre of Excellence in Tallinn (Lang 2008, p. 6).

Due to the political circumstances Estonian officials accused the Russian government to be responsible for the attacks while Moscow denied having any connections to it. Estonian Foreign Minister Urmas Paet and Minister of Justice Rein Lang both declared that IT analysis had proven the involvement of Russian government computers in the attacks. In this context they also mentioned the involvement of Russian Presidential administration networks in the attacks (Spiegel Online 2007c).

Besides single cases of web defacement on governmental websites, DoS attacks were the main method used to interfere with Estonian infrastructure. Before and during the attacks, in several Russian web-forums so called patriotic hackers informed users (especial the younger generation, the script kiddies) how to participate in cyber attacks on Estonia. Driven by patriotic outrage there was a growing number of young Internet users in Russia wanting to harm Estonia by attacking its infrastructure. Nevertheless the most serious attacks were the ones that had botnets involved controlled by more advanced attackers. Botnets used during the attacks consisted of drones from several countries including the USA, Brazil, Russia, Canada, Egypt, Peru, and Vietnam. This way hundreds of thousands of computers were guided to attack specific points at the same moment. IT analysts observing the attacks discovered that concentrated attacks started and ended at fixed points of time (after exactly two weeks) proving the use of botnets. Also the qualitative level of the more serious attacks pointed out that professional hackers were behind them (Davis 2007). Additionally, some of the attacks happening during the day stopped at midnight (Faz.net 2007). This fact suggested that hired botnets (which are usually paid per day) were in use which implies high costs for the attackers that can barely be carried by individual Internet users. Furthermore analysts from the IT security company Arbor Networks discovered, that some of the botnets used against Estonia were just a few weeks earlier employed to disturb the IT presence of an alliance of Russian opposition parties (Davis 2007).

Estonian officials constantly blamed the Russian government to be responsible for the attacks, but this accusation could never been proven. Russia always denied having any responsibility but hardly considered to clear up the occurrences by activating its secret service FSB. Due to the SORM II regulation, the FSB has control over all Internet traffic in Russia. Although SORM II was developed to control the Internet for security reasons President Putin (a former FSB director) did not initiate an investigation.

In January 2008 a 20-year-old Russian Estonian was arrested and fined in the Baltic republic for conducting cyber attacks on Estonian infrastructure (Kirk 2008). However, the facts presented above make clear that highly sophisticated actors were behind the attacks and not a group of patriotic script kiddies. After two years without further clarifying information, Russian State Dume Deputy and member of the Russian delegation to the Parliamentary Assembley of the Council of Europe (PACE) Sergei Markov (accidentally) revealed that one of his assistants was responsible for (at least part of) the cyber attacks. This man was later identified as Konstantin Goloskokov, a leading member of the Nashi youth movement, an organization founded by Putin supporter Vladislav Surkov in March 2005. Goloskokov confirmed his responsibility in the attacks. In an interview given to the Financial Times in March 2009 he stated that he and other members of his organization simply accessed Estonian websites until they crashed (Clover 2009). In the interview he pointed out that all activities were undertaken without governmental instructions or support.

Considering the impact of the cyber attacks it is unlikely that Goloskokov and his colleagues brought down the infrastructure of the whole country just by accessing websites. More interesting is to consider the possibility of Nashi being involved in concentrated botnet attacks. The organization had more than 120.000 members in 2008 and is famous for its street activities against Russian opposition parties (Heller 2008). It was also involved in violent protests against the Estonian embassy in Moscow in May 2007. Estimations by the German Institute for Peace Research and Security Policy say that the Putin administration supported Nashi and other youth organizations with several 100.000 U.S. dollar per month. Nashi's annual summer camp had an estimated budget of 6-7 million U.S. dollar (idem). Considering the costs for hiring extensive botnets how they were used against Estonia, Nashi exhibits not only strong motivation and confessing members but also possesses the necessary financial resources.

4.4.1.2 Georgia

The cyber attacks in July and August 2008 against Russia's neighboring republic Georgia happened in the context of the enduring conflict between the two countries over South Ossetia (Closson; Halbach 2008). The legal status of this Caucasian region has been the reason for disputes and military confrontations for several generations in history. During the times of the Soviet Union Moscow's constant support for new Ossetian settlements and a parallel relocation of Georgians from the region lead to a growing Ossetian population which today is about 66% in South Ossetia compared to 29% Georgians. It remained an autonomous region within the Georgian Soviet Socialist Republic until 1990 when it declared its independence which was not recognized by any other state. Since then Georgia claimed the region as part of its own state (independent since 1991) and is supported by the majority of states of the international community. Moscow supported South Ossetia's demand for independence and offered Russian citizenship to the inhabitants of the region for which reason about 90% of the population in South Ossetia is today formally Russian.

Figure 4: Map of Georgia and Caucasus Region

Source: BBC Online

Since the 1990s the conflict in the region resulted in numerous military disputes which were interrupted by phases of relative peace which was common also in other Caucasian countries after the end of the Soviet Union and described by researcher as “frozen conflict“ (Borgen 2009). Others questioned this term arguing that South Ossetia and also Abkhazia showed continuously violent clashes between rivaling actors (König 2006). In August 2008 intensified clashes of the preceding months lead to an occupation of South Ossetia by Georgian troops, followed by a Russian invasion in South Ossetia and parts of Georgia as well as bombings of several Georgian cities (Closson; Halbach 2008). After the withdrawal of Georgian troops a few days later, Russia officially recognized South Ossetia's (and Abkhazia's) independence in August 2008, later followed by Nicaragua (September 2008) and Venezuela (September 2009). This step can be interpreted as a consequence of the independence of Kosovo, accepted by a number of Western states in February the same year, which was emphatically criticized by the Russian government being still concerned about independence struggles of a number of territories in the former Soviet region.

While violent outbreaks between Georgia and Russia had been a recurring phenomenon of the region since the early 1990s, the fights in August 2008 added a new component to the conflict. Already before the occupation of South Ossetia started in August, virtual attacks were launched against several parts of the Georgian infrastructure. These attacks, which started in July 2008 (Adair 2008), included DDoS attacks, botnets, logic bombs[38] and other measures. Affected were mainly the President's office and other governmental networks, financial networks, news services, and the U.S. embassy. Before and during the virtual aggressions, potential targets were published on several Russian online discussion forums to mobilize patriotic hackers like it had happened in the Estonia attacks the year before. A large number of websites targeted was blocked for several days. Some governmental sites were moved to Turkish and U.S. American servers to continue informing provisionary about the armed conflict in South Ossetia. The Ministry of Foreign Affairs continued publishing information on a blog after its own network broke down (Waterman 2008). Also cell phone services broke down as a consequence of the attacks on financial networks (Corbin 2009). To secure their own networks, foreign banks cut their connections to Georgian banks, leaving them isolated from the global financial system. Besides the Georgian networks, also in Russia and South Ossetia virtual attacks on critical infrastructure took place, albeit to a lesser extend.

[38] A logic bomb is a piece of code which can be placed within a chosen part of an adversary's IT infrastructure to be activated at a strategic moment of time. Once activated the code can harm the adversary's IT system from the inside.

Joseph Nye later pointed out that never before, armed conflicts and virtual attacks had happened in combination: “The Russia-Georgia conflict represents the first significant cyber attacks accompanying armed conflict. Welcome to the twenty-first century.“ (Nye 2008). Although as stated above, already the Kosovo conflict saw a combination of cyber war measures and traditional armed aggressions, Nye is right that the Caucasus war 2008 included cyber measures on an intensified level compared to the Kosovo war in 1999.

Similar to the attacks on Estonia, also the Georgian government accused Moscow for being responsible for the breakdown of governmental and civil infrastructure. Moscow again denied its responsibility. There are different possible scenarios for who conducted virtual attacks on Georgia. They range from patriotic hackers over criminal organizations to the governmental level.

The involvement of patriotic hackers and script kiddies in virtual attacks against Georgia is a widely accepted fact. Corresponding discussions in Russian online forums including instructions by experienced hackers and the supply of the necessary tools, but also the results of different IT security analysis have proven this to be true. Also the ongoing virtual attacks after the Russian government had officially ended its military campaign support this argument. Beyond that the Shadow Foundation, an organization specialized in Internet security research, had watched a number of servers for an extended period of time (some for more than one year) before the same servers became involved in the Georgia attacks. As those servers had been used before August 2008 to commit ordinary criminal activities which, following the researchers, were not connected to the Russian government, they concluded that the servers mentioned were rather used by individuals or criminal organizations (Johnson 2008). Although it could be possible to hire these services also with public resources.

Looking at the participation of criminal organizations the situation becomes more complex. Besides providers of botnets, who can be considered cybercriminals as well, also the Russian Business Network (RBN) is a potential actor being involved in the attacks. As stated above, the network functions as a non-registered company which is responsible for a high percentage (approximately 60%) of all cybercrime activities worldwide (Warren 2007). In spite of its activities the RBN, operating from St. Petersburg, was never charged by Russian authorities. Its probable relations to political officials might be one of the reasons (idem). Nevertheless the network

disappeared in November 2007 and has since then been spotted on different locations outside of Russia, where the lack of IT policies and legal regulations facilitate their activities. The involvement of cybercriminal organizations in the attacks on Georgia and a certain level of cooperation with Russian officials were also confirmed by the U.S. Cyber Consequence Unit's report handed to the U.S. government in August 2009 (Kirk 2009).

Looking at the governmental level it is unlikely that the Kremlin was directly involved in any cyber attacks on Georgia. Although some aspect indicate that officials from the (lower) political spectrum and the military could have been involved or at least have cooperated with virtual attackers. One example is the coordination of timing and location of both virtual and military strikes. On 9 August 2008 cyber attacks that brought down news service stations in the Georgian city of Gori happened just moments before the Russian air-force bombed strategic goals in the same city (Goodwin 2008). This indicates a certain form of cooperation to prevent the spreading of information after the bomb attacks. Another indicator is the involvement of the two government-controlled telecommunication companies Rostelecom and Comstar. Servers of both companies were identified having blocked Internet traffic going to Georgia as well as launching DDoS attacks against the country (Leyden 2008).

4.4.2 China

The role of China in international telecommunication is seen as a complex and also complicated issue. In 2010 China had more than 400 million Internet users (Internet World Stats 2010). Due to its population size this number referred to just about one third of the country's inhabitants, mainly situated in the urban centers of the country. While ICT companies and analysts see China as the market with the biggest growth potential for further investments, global civil society organizations and foreign (mainly Western) governments regularly complain about national Internet filter and censorship as well as constantly occurring cyber attacks. Different than in the Russian case, cyber attacks from China have so far not targeted foreign networks in the same complexity and with comparable destructive results like in Estonia or Georgia. They were rather concentrated on individual networks in different countries often with the intention of spying.

Early cases of cyber attacks from China go back to the end of the 1990s. As a response to a massive demonstration of Falun Gong members in Beijing in April 1999, a number of servers in the USA, Canada and the UK hosting websites of the movement fell victim to cyber attacks (Wacker 2000, p. 36). In the same year cyber attacks happened on U.S. networks after the bombing of the Chinese embassy in Belgrade. In this context it is interesting to mention, that at this time the Internet was a relatively new network that was used only by a small percentage of the population, a big part of them being university members. In December 1999 only 3,5 million computers in China had access to the Internet. They were used by an estimated number of 8,9 million people, less than 1% of the whole population (Wacker 2000, p. 11).

Over the years more similar attacks occurred that were connected to particular events like an airplane accident involving two machines from China and the USA, causing the death of the Chinese pilot in April 2001 (the Hainan Island incident). This crash resulted in massive cyber attacks from China on U.S. governmental networks and vice versa (Smith 2001). The attacks were conducted by patriotic Chinese and American hackers which openly declared responsibility on the net. While this “First World Hacker War“ (Smith 2001), which caused serious damage to parts of American critical infrastructure (Cornish 2009, p. 14), was based on mutual cyber activities, in the following years China conducted more secret cyber attacks, targeting public institutions in different countries with the intention to illegitimately transfer information to their own networks.

Between 2005 and 2010 especially Western industrialized countries discovered virtual attacks on their governmental networks. In most cases the attackers tried (often successfully) to access public networks like the British Foreign Office, the U.S. Pentagon, or the German Ministry of Exterior and others. In the majority of the cases mentioned, the attacks were traced back to Chinese networks, in some cases even directly to the Chinese Army (Norton-Taylor 2007). U.S. investigators suspected a Chinese espionage ring they called Titan Rain to be responsible (Thornburgh 2005). Alex Neill, Asian security analyst at the British Royal United Services Institute, declared the attacks could be part of the “pressure point warfare“ strategy of China's Army to weaken its opponents by “attacking...specific nodes to leave the adversary paralysed“ (Norton-Taylor 2007).

James Lewis from the Center for Strategic and International Studies in Washington DC is skeptical. Following his analysis the Chinese networks' vulnerability could attract third parties with the intention to attack foreign infrastructure and let investigators fall into the easy trap of (post-) Cold War logic:

> In the 1980s the Americans looked under their beds and believed they saw the KGB; now they believe they see the PLA [Peoples Liberation Army]. A hostile service from a third country might be drawn to use Chinese computers to launch an attack hoping that our proclivity to ascribe bad intent to China would cloud any investigation. (Lewis 2005, p. 2).

Furthermore, Lewis pointed out that also China's officials would have used the way over a third country instead of leaving a trail back to their own networks. He suggested that cybercriminals could be responsible for virtual attacks on governmental networks to sell the information to any secret service that is willing to pay.

The most extensive cyber attack that was traced back to Chinese computers was discovered by researchers at the Munk Centre for International Studies at the University of Toronto and the Information Warfare Monitor. The results of their 10 months lasting research (June 2008 - March 2009) were published in March 2009. Initial point of the research was a request by the Office of the Dalai Lama to search its networks for probable malware. The infiltration of the office computers was assumed after Chinese officials proved to hold information about Tibetan exile politicians that they most probably had received through the Internet. During the investigations the researchers discovered that a large number of computers of the Tibetan community had been infiltrated by trojans which opened up the systems for intruders offering them access to content stored in the respective networks. Besides that the attackers created the possibility for them to gather information by enabling microphones or webcams on the infiltrated computers (Deibert; Rohozinski 2009, p. 34).

During the investigations the researchers discovered that besides Tibetan also a large number of other computers were connected to what they called the GhostNet. Between May 2007 and March 2009 at least 1295 computers from 103 countries were infiltrated by the espionage network (idem, p. 40). 30% of the networks attacked were considered by the researchers to be “high value targets“ like ASEAN and NATO networks, embassies and foreign and other ministries of

several countries like Bangladesh, Brunei, Germany, Indonesia, Pakistan, Portugal, South Korea, Taiwan and Vietnam, as well as news organizations, universities and private companies in Hong Kong, India, Russia, USA and more. A strong focus was on governmental networks in South and South East Asia.

Tracing back the attackers, the researchers found out that 70% of the servers controlling GhostNet activities against Tibetan networks were located in China (idem, p. 22). The rest was dispersed over different countries among them Sweden, Taiwan and USA. Also a vast amount of servers attacking non-Tibetan goals were located in China. In this context it is interesting to notice that several servers were situated on the Chinese Hainan Island where intelligence and technical army facilities reside. Moreover the concentration on political, economic and military targets in South and South East Asian countries indicates that Chinese officials could be the operators of GhostNet. Nevertheless the report of the Information Warfare Monitor concludes that the necessary tools to built up espionage networks are available on the net and not exclusively accessible by military or secret service officials. Also cybercriminals could build similar networks to gather and sell information, although GhostNet has a strong political character compared to formerly discovered criminal networks. What in turn suggests a non-responsibility of Chinese officials is the argument also brought up by James Lewis before, stating that other actors could have built GhostNet using Chinese infrastructure to lead investigators on the wrong track.

Considering the cautiousness of the report concerning responsible persons behind the virtual attacks, it is remarkable to compare it to a second one, composed by two researchers from the University of Cambridge who also have been involved in the research on GhostNet. In *The Snooping Dragon*, Shishir Nagaraja and Ross Anderson give a different point of view about the origins of GhostNet. They clearly state the responsibility of the Chinese government to attack Tibetian networks. In the first sentence of the abstract they introduce their paper as treating “a case of malware-based electronic surveillance of a political organization by agents of a nation state.“ (Anderson; Nagaraja 2009, p. 3). They further claim that the “surveillance attack [was] designed to collect intelligence for use by the police and security service of a repressive state...“ (idem). In their conclusion they amplify this aspect by pointing out: “People in Tibet may have died as a result.“ (idem, p. 11).

The comparison of GhostNet and Titan Ring (and a number of smaller incidents mentioned above) to the cyber attacks on Estonia and Georgia show that cases involving Chinese networks as the source of the attack are more likely to involve espionage rather than causing damage to a foreign network. Nevertheless, also individual hacker activities can be traced back to Chinese networks which in the past (e.g. in times of Chinese-American tensions) aimed at corrupting foreign infrastructure. Although there is no direct financial interest behind such activities they must be considered a cybercrime as well. Furthermore, James Lewis' assumption regarding the exploitation of weak points in the Chinese infrastructure by cybercrime groups underlines the possible correlation between political cyber attacks and cybercrime. These relations become even clearer when looking at widely spread DDoS attacks which depend on huge botnets to be successful. The involvement of illegitimate networks provided by ordinary cybercrime groups like the Russian Business Network and other less known groups prove the existence of an intersection of cybercriminals and politically motivated cyber attackers. Also the involvement of the Russian pro-Kremlin organization Nashi in the attacks on Estonia in 2007 proves that relation. In fact, there are two possible scenarios for Nashi's involvement in cybercrime. Given the fact, that cyber attacks on Estonia started shortly after the spontaneous demonstrations on the streets of Tallinn, the attackers must already have had contacts to cybercriminals beforehand to instantaneously rent vast botnets. A second scenario includes the possibility of the attackers possessing their own botnets which they used during the attacks. This indicates that they have been involved in cybercrime activities or its preparations before the incidents in Estonia.

Independently of time and location it can be stated that a protection against politically motivated cyber attacks postulates a protection against ordinary cybercrime. To succeed in this question a focus on the international level is indispensable. In an interview with the author, Dayton Law School Professor Susan Brenner stressed that “purely parochical, national solutions cannot address this type of stateless criminal activity, which by implication means that multilateral/international solutions are needed“ (Brenner 2011). Due to its transnational character cybercrime is hardly controllable on a national level but requires international cooperation. For this reason a number of international organizations and other international actors are striving for international agreements and regional regulations.

4.5 International Actors

There is a large number of international and regional actors involved in cybercrime debates. However, little research (in fact, almost none from an international relations approach) has been conducted so far concerning this international level. Each of the organizations mentioned in this chapter could be the object of an individual research project. To remain focused on the objective of this thesis, a deeper analysis of each actor is not possible at his moment but can be considered for future research projects. The following paragraphs will give an overview about the activities of international organizations in the global cybercrime scenario.

4.5.1 Council of Europe

The Council of Europe (CoE) started focusing on cybercrime issues already in the 1970s during a number of conferences. In 1985 the first expert committee was set up to discuss the questions of computer-related crimes. After almost ten years of different reports and recommendations on cybercrime, the European Committee on Crime Problems (CDPC) built a new committee of experts with the specific goal to develop a convention on cybercrime. Between 1997 and 2000 the committee continued working on its task until during an official signing ceremony on 23 November 2001 in Budapest the Convention on Cybercrime (also called Budapest Convention) was adopted. Among the 30 countries signing the convention on that day were also four non-members of the CoE which had been involved in the development process: Canada, Japan, South Africa, USA. The convention entered into force on 1 July 2004. Following the CoE website, another 16 states had signed the convention by October 2010, making a total of 46 states.[39] "Surprisingly few" as Susan Brenner put it (Brenner 2011). Following her analysis:

> (…) some of the reticence to move toward multilateral/international solutions is a function of what [she sees] as an increasingly dated presumption that the nation-state systems which have historically dealt with crime (and terrorism and war) are quite capable of dealing with

[39] The CoE website listed the following countries as having signed the Budapest Convention by December 2010: Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxemburg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, F.Y.R.O. Macedonia, Ukraine, United Kingdom, USA.

cyberthreats. (idem).

An additional protocol that states could chose to sign is the Protocol on Xenophobia and Racism (CoE 2003). During the development of the convention the inclusion of statements on xenophobia and racism were separated from the convention as some of the participating countries (e.g. USA) articulated concern about the restriction of the right to freedom of speech. To not let different perceptions on this topic endanger the completion of the convention, the respective paragraphs were therefore separated from the text of the treaty. To foster support for the convention, the CoE offered cooperation projects to countries interested in preparing their legislation for the necessary standards to sign the treaty. One example is a joint project of the CoE and Georgia which started in June 2009 (CoE 2009).

4.5.2 G8

Early activities of the G8 against cybercrime can be found in the establishment of the Financial Action Task Force (FATF) which was founded during the Paris Summit of the then G7 in 1989. The focus of the FATF was to develop norms and standards for governments and financial institutions to combat international money laundering. In 1990 the FATF published its Forty Recommendations, a set of measures for states and banking institutions to support their efforts against money laundering which were updated over the years (FATF 2003). Within these guidelines the FATF stressed that criminal activities in the financial sector also happened via the Internet. Especially mentioned were the cases of online gambling. Later, the problem of gambling in cyberspace was picked up again in a special report (FATF 2009).

In 1996 during the G7 Summit in France the Lyon Group was set up which consisted of a number of G7 senior experts on international crime. One of its early tasks was to revise the Forty Recommendations. Furthermore the group became involved in the development of several documents and recommendations towards cybercrime prevention. Its efforts can be found already in the G7's 1997 statement of ten principles and the action plan to combat high-tech crime (G8 1997). In these documents the G7 concluded, inter alia, that transborder cooperation was necessary to successfully combat cybercrime (at that time also labeled as high-tech crime) and that law-

enforcement personnel had to be trained in this regard. In the Action Plan they stimulated the creation of a 24/7 Point of Contact Network which was based on the idea of the Subgroup on High-Tech Crime, one of five subgroups of the Lyon Group.

The Subgroup (or Subcommittee) on High-Tech Crime was responsible for the creation of the Critical Information Infrastructure Protection Directory (CIIP) and the publication of several documents and international recommendations towards cybercrime protection. It furthermore created the 24/7 Network of High Tech Points of Contact (also known as the 24/7 Network of Contacts for High-Tech Crime). This network can be considered as a crucial contribution of the G8 to combat cybercrime. Its central idea was to build up a network of contact points for transnational investigations in all participating countries which are available 24 hours per day. After the network had been established, more than 40 other countries joined it. The idea was later picked up as well in the Budapest Convention on Cybercrime.

In 1999 the G8 agreed on its Communiqué on Combating Transnational Organized Crime which affirmed the establishment of the 24/7 network and also included a special passage on high-tech crime mentioning explicitly child exploitation, financial crimes and attacks on critical infrastructure (G8 1999). Furthermore it stressed the necessity of improving national legal systems to combat cybercrime. In 2002 the G8 came up with its Recommendations on Transnational Crime which included two sections on high-tech crime and child offense on the Internet (G8 2002). After 2002 the G8 continuously underlined the importance of the combat against cybercrime, for example during their Washington meeting in 2004 or the Moscow meeting in 2006 (G8 2004; G8 2006). However, since the 9/11 attacks many cybercrime (or high-tech crime) issues discussed by the G8 so far are now discussed within the cyberterrorism context. For this reason already in 2001 the Lyon Group on international crime was combined with the Roma Group on fighting international terrorism.

4.5.3 United Nations

Within the United Nations (UN) system different organizations addressed the problem of cybercrime in the past. The first UN publication explicitly focusing on cybercrime is the UN Manual on the Prevention and Control of Computer-Related Crime which was published in 1994 (UN 1994). This manual can be seen as a result of the 8th UN Congress on the Prevention of Crime and the Treatment of Offenders which took place in Havana in 1990. Already in the Report of the Asia and Pacific Regional Preparatory Meeting in 1989 it was pointed out that "risk analysis to assess vulnerability to ... computer crime ... had an important role to play in taking preventive countermeasures or making the commission of crime more conspicuous." (UN 1989, p. 19). During the congress a resolution (proposed by a Canadian representative) was adopted which inter alia called for the modernization of national criminal laws, the improvement of computer security, the adoption of measures to sensitize the public, the adoption of adequate training measures for judges, and the elaboration of ethical computer rules (UN 1994, paragraph 18).

In December 2000 the General Assembly of the United Nations (UNGA) passed the Resolution on Combating the Criminal Misuse of Information Technologies (UN 2001) in which it appreciated the results achieved so far while at the same time stating several aspects necessary to further improve the efforts of anti-cybercrime measures, being:

- elimination of safe havens for cybercriminals by improving national legislations ("safe haven" is a term used in many international cybercrime documents)
- international cooperation among states regarding law enforcement and information exchange
- adequate training of law enforcement personnel
- data protection
- permission for criminal investigators to access data for investigational reasons
- public awareness building
- combination of privacy and individual rights preservation with effective criminal investigations.

In a following resolution from December 2001, the UNGA referred to the UN Commission on Crime Prevention and Criminal Justice within the United Nations Office on Drugs and Crime (UNDOC) as a recommendable source of anti-cybercrime activities (UN 2002a).

In March 2001, the UNDOC commission published its Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime, conducted due to a request by the Economic and Social Council (ECOSOC) in 1999 (UN 2001). In this report the commission analyzed the nature of computer-related crimes and its costs before declaring the necessity of technical assistance for states that are not yet accustomed to the prevention of cybercrime. Furthermore it recommended the development of a more detailed analysis of the problem whose results were to be presented at the 11th session of the Commission on Crime Prevention and Criminal Justice in 2002.

During the 10th session of the commission in 2001 the plans for a deeper analysis were supported by most speakers. In the report of the session, actions against high-technology and computer-related crime on the national and international level were demanded, among them the general criminalization of ICT-related crimes, the inclusion of the ICT industry in cybercrime discussions, the fostering of research on cybercrime and the promotion of international cooperation projects. This list of demands and recommendations is called the Plan of Action against High Technology and Computer-Related Crime and was later published again in resolution 56/261 by the General Assembly in April 2002. As the report of the 11th session of the commission called Effective Measures to Prevent and Control Computer-Related Crime (April 2002) suggested, the further research project announced in 2001 was not conducted due to lack of financial resources (UN 2002b).

In April 2010 the 12th UN Congress on Crime Prevention and Criminal Justice met in Salvador (Brazil) where participants discussed the possibility of a new global cybercrime treaty. The wish for this new agreement was expressed by a number of states (among them Russia, China and several developing countries) that declared their dissatisfaction with the Budapest Convention which at that time was almost ten years old and in their opinion did not address the latest challenges (e.g. cloud computing) and was interfering with the concept of national sovereignty by giving police agencies the opportunity to investigate in foreign countries' networks. Besides that, Russian

supporters of a new global approach underlined, that the previous convention had been developed by few Western states while an international UN-based approach would be more appropriate to include concerns and requests from other states as well. European representatives, the USA and other supporters of the Budapest Convention made clear, that a new treaty would be unnecessary and suggested the inclusion of new issues into the existing document. In the final declaration (Salvador Declaration) the participants of the congress agreed to form

> an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime. (UN 2010).

4.5.3.1 International Telecommunication Union

As the UN's main agency for telecommunication the International Telecommunication Union (ITU) plays an important role in cybercrime prevention as well. In 2007 it announced a two year plan to reduce cybercrime, called the Global Cybersecurity Agenda, GCA (ITU 2007). The five pillars of the CGA are:

1. Finding technical solutions for every environment
2. Developing interoperable legislative frameworks
3. Building capacity in all relevant areas
4. Establishing appropriate organizational structures
5. Adopting effective international cooperation mechanisms

Together with the American Bar Association (ABA) the ITU developed a Toolkit for Cybercrime Legislation that was first presented in May 2009 before a revised edition came out in the following year (ITU 2010). The intention of the toolkit was to assist governments in developing effective legislations to prevent and combat cybercrime.

4.5.3.2 Others

While the documents mentioned in the paragraphs above are the central UN outputs on cybercrime, there are several others that deal with the problem or at least include passages referring to computer-related crimes. Among them are the WSIS documents Geneva Plan of Action and the Tunis Agenda for the Information Society.

Others include, as listed in the ITU Global Strategic Report (ITU 2008):

- CCPCJ 2007 Resolution 16/2 of April 2007 “Effective crime prevention and criminal justice responses to combat sexual exploitation of children” (especially paras 7, 16).
- ECOSOC Resolution E/2007/20 of 26 July 2007 on “International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime” (E/2007/30 and E/2007/SR.45).
- ECOSOC Resolution 2004/26 of 21 July 2004 on “International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes”.
- Para. 18 of the “Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century”, endorsed by General Assembly Resolution 55/59 of 4 December 2000 and Para. 36 of “Plans of action for the implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century” annexed to General Assembly Resolution 56/261 of 31 January 2002.
- Paras. 15 and 16 of Bangkok Declaration on “Synergies and Responses: Strategic Alliances

in Crime Prevention and Criminal Justice", endorsed by GA Resolution 60/177 of 16 December 2005.

- Recommendations by an Ad-hoc Congress Workshop on "Measures to Combat Computer-Related Crime", held in Bangkok on 22 April 2005 as part of the Eleventh UN Congress on Crime Prevention and Criminal Justice. Para. 2 of General Assembly Resolution 60/177 invites Governments to implement all recommendations adopted by the Eleventh Congress.
- General Assembly Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on "Combating the criminal misuse of information technologies". The latter resolution invites Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, inter alia, the work and achievements of the Commission on Crime Prevention and Criminal Justice.
- Commission on Narcotic Drugs Resolution 48/5 on "Strengthening international cooperation in order to prevent the use of the Internet to commit drug-related crime".
- Para. 17 of General Assembly resolution 60/178 of 16 December 2005 on "International cooperation against the world drug problem".
- Commission on Narcotic Drugs Resolution 43/8 of 15 March 2000 on Internet.
- ECOSOC Resolution 2004/42 on "Sale of internationally controlled licit drugs to individuals via the Internet".
- Various conclusions and recommendations of subsidiary bodies of the Commission on Narcotic Drugs (e.g., the Sub-Commission on Illicit Drug Traffic and Related Matters in the Near and Middle East and regional HONLEA meetings).
- The International Narcotics Control Board (INCB) published recommendations in 2005 to curb the spread of illicit sales of controlled substances, particularly pharmaceutical preparations, over the Internet. INCB is also finalizing a set of guidelines on this.
- General Assembly Resolutions 57/239 of 31 January 2003 and 58/199 of 30 January 2004 on "Creation of a global culture of cybersecurity", which invite Member States to take note of ongoing cybersecurity collaboration and to promote a culture of cybersecurity.

4.6 Regional Actors

4.6.1 Asia-Pacific Economic Cooperation

The driving force regarding cybercrime issues within the Asia-Pacific Economic Cooperation (APEC) is the Telecommunication and Information Working Group (TEL), which was founded in 1990. It is responsible for all aspects of information society within the organization, ranging from reducing the digital divide over implementing e-government structures to developing capacity building programs. On its 1999 meeting in Lima TEL included ICT security and critical infrastructure protection into their agenda.

On 21 October 2001 APEC launched a Statement on Counter-Terrorism in which also the protection of critical infrastructure and telecommunication networks was emphasized (APEC 2001). Five months later the APEC Telecommunication and Information Ministers presented the Shanghai Declaration on 30 May 2002 (APEC 2002b). This declaration underlined the necessity of a secure IT environment for economic growth and expressed the commitment of the APEC members to improve network security. While the Shanghai Declaration does not explicitly include any reference to cybercrime, the two attached documents do. The Program of Action, included in annex A, mentioned the importance of the UN resolution 55/63 (Combating the Criminal Misuse of Information Technologies) and recommended its implementation within the APEC states (APEC 2002c). In annex B the ministers noted the importance of the Cybercrime Convention of the Council of Europe and the OECD Guidelines for the Security of Information Systems (APEC 2002d).

During the 14th Ministerial Meeting of APEC in Mexico (October 2002), TEL introduced a recommendation for an APEC Cybersecurity Strategy (APEC 2002a). It recommended again the implementation of the UN resolution 55/63 and referred also once more to the CoE Convention on Cybercrime as a positive example for APEC states to adapt their national legislation to computer-related crimes. It moreover recommended the formation of IT security units (similar to CERT) and encouraged APEC members to join the G8 24/7 Point-of-Contact Network. Other initiatives the strategy referred to are the OECD Guidelines for the Security of Information Systems and finally it urged its members to develop cybercrime prevention training programs. In March 2003 the APEC Cybersecurity Strategy was adopted during the 27th APEC meeting in Kuala Lumpur. To strengthen

APEC member states in dealing with cybercrime, TEL set up a number of training activities by itself like Asia Pacific Computer Emergency Response Team (APCERT) Exercises in 2009 and the APCERT Drill in 2010 as well as a number of bilateral cybercrime legislative workshops (APCERT 2011).

4.6.2 Commonwealth of Nations

The Commonwealth of Nation's efforts to prevent and reduce cybercrime are strongly related to the Model Law on Computer and Computer Related Crime, passed in October 2002 (Commonwealth of Nations 2002). The Model Law was developed by the Expert Group on Computer Crime and Related Criminal Law Issues which from the early beginning oriented their work on the Budapest Convention on Cybercrime. It concentrated mainly on the issues of:

- illegal access,
- interference with data,
- interference with computer systems,
- illegal interception of data,
- illegal devices, and
- child pornography.

Due to its orientation on the widely accepted CoE Convention, the Model Law was appreciated by the member states of the Commonwealth. The discussion on cybercrime prevention measures did therefore proceed on a more consistent way than in other regions or organizations. Nevertheless, in 2010 several member states still needed to adapt their national legislation to the standards of the Model Law. For this reason the Expert Group continued its work developing recommendations to improve domestic law with the objective to implement the CoE convention. To further promote the debate on cybercrime the Commonwealth Cybercrime Initiative was founded which played an important role during the preparation of the 2011 IGF in Kenya. One of the main

objectives of the initiative is the continuing support for the Budapest Convention and the preparation of the Commonwealth's associate states to adapt national legislation in this regard (Commonwealth of Nations 2011).

4.6.3 European Union

In March 1998 the European Union (EU) recommended its members to adopt the G8 24/7 Point of Contact Network (Council of the European Union 2001). In a 2001 communication (Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime*)* the European Commission addressed the questions of privacy offense and content-related offense, economic crimes, unauthorized access, sabotage and intellectual property offense and recommended the improvement of national legislations to adapt to growing online crime (European Commission 2001). Especially mentioned in this context are child offense, racist content, hacking and denial-of-service attacks.

In 2002 the Commission also developed the Framework Decision on Attacks against Information Systems, which was later adopted by the European Council in February 2005 (Council of the European Union 2005). In this document the EU member states are requested to take necessary measures in the prevention of cybercrime, especially concerning their legislations in the respect of unauthorized access to information systems as well as unauthorized damage of information systems and data.

In 2007 the European Commission published another communication called Towards a General Policy in the Fight against Cyber Crime (European Commission 2007). In this document the Commission gave a general overview about the current situation and forms of cybercrime activities aiming especially at child offense, racist and xenophobic content, terrorism and other violent activities. It stressed the necessity to protect critical infrastructure and to enhance cooperation among the member states of the EU. Furthermore the communication includes an overview over the latest EU and international measures to combat cybercrime. In the concluding recommendations the commission underlined, inter alia, the importance of providing financial

resources to prepare law enforcement and judicial authorities for the new challenges, to develop research initiatives investigating computer-related crimes and to enhance international cooperation and the dialogue with the IT industry.

After a number of major virtual incidents like the attacks on Estonia and Georgia it became clear also to the European Union that botnets were to be among the most crucial tools for cybercriminals in the coming years. In this context the EU intensified its focus on the criminalization of botnets and other tools used to infiltrate information systems. In 2010 the European Commission published a proposal to discuss this problem in the European Parliament. The document underlined:

> There is evidence of a tendency towards increasingly dangerous and recurrent large scale attacks conducted against information systems which are critical to states or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated tools that can be used by criminals to launch cyber-attacks of various types. (European Commission 2010a, p. 10).

This document is the first step in a new challenge the European Union is heading for. So far, there are no specific ideas about how to realize this project. A much more concrete plan is the installation of a European Cybercrime Center until 2013 “to build operational and analytical capacity for investigations and cooperation with international partners“ (European Commission 2010b, p. 9).

4.6.4 Organization of American States

Since 1999 the Organization of American States (OAS) has the debate on cybercrime on their agenda. In March that year the OAS meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA) decided to set up a group of experts on cybercrime. In the final report of their meeting in Lima, REMJA declared that an informal working group on

cybercrime had developed a draft recommendation demanding the forming of an intergovernmental expert group to investigate computer-related criminal activities, national policies and legislations in respect to these activities, as well as possible cooperative activities of the member states, and to report about their findings to the next REMJA meeting (OAS 1999).

In March 2000 the report of the Group of Governmental Experts on Cybercrime was presented during the 3rd REMJA meeting in Costa Rica and its main points were included in the final report of the meeting (OAS 2000a; OAS 2000b). In the conclusion the ministers urged the member states to enhance efforts in cybercrime prevention and prosecution by identifying authoritative agencies within their countries, adapt national legislations, facilitate international cooperation, develop training measures, and consider participation in the G8 24/7 Point-of-Contact Network.

At the REMJA IV meeting in Trinidad and Tobago in March 2002 it was confirmed that the Group of Governmental Experts on Cybercrime should continue its work to

> consider the preparation of pertinent inter-American legal instruments and model legislation for the purpose of strengthening hemispheric cooperation in combating cyber-crime, considering standards relating to privacy, the protection of information, procedural aspects, and crime prevention. (OAS 2002, p. 35).

In the following years the Group of Governmental Experts met in 2003, 2006, 2007 and 2010, continuously monitoring progress made by OAS member states in regard to their recommendations.

4.6.5 Organization for Economic Cooperation and Development

The Organization for Economic Cooperation and Development (OECD) is one of the pioneers among international organizations when it comes to putting computer-related crimes on its agenda. Already in the early 1980s first research projects were developed to investigate the back

then relatively new phenomenon of computer crime. In 1986 it published an analysis of legal policies in the OECD area towards computer-related crime (OECD 1986).

In 1990 an expert group was set up by the OECD Information, Computer, and Communications Policy Committee (ICCP) to develop guidelines for information security. Later in 1997 these guidelines, which had been adopted by the OECD Council already, were revised and served as a basis for the OECD Guidelines for the Security of Information Systems and Networks, adopted in 2002 (OECD 2002). The principle goals the OECD outlined in the beginning of the document were:

- the promotion of a culture of security,
- raising awareness about the risk to information systems and networks,
- fostering confidence among network participants,
- creating a frame of references to understand security issues,
- promoting cooperation and information sharing,
- promoting security as an important objective.

In 2005 an additional report on spam and its impact on developing economies was published by the OECD Task Force on Spam (OECD 2005a). In the same year the OECD presented another cybercrime-related document called The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries (OECD 2005b). This document focused on the national efforts made since adoption of the OECD Guidelines in 2002.

In 2010 researchers of the Oxford Internet Institute and the London School of Economics investigated current global cybersecurity risks within the OECD Future Global Shocks Project. They came to the conclusion that cyberwar which in the past years became an issue of growing importance especially for the military sector was unlikely to happen in a seriously threatening dimension. However, they emphasized that the technical measures which are usually mentioned within the discourse on cyberwar (and which they called cyberweapons) were basically the same measures used to conduct cybercrimes (Sommer; Brown 2011).

4.7 Civil Society and Cybercrime

The problem of cybercrime is a problem of security that affects all parts of society. As shown before, government infrastructure suffers from cyber attacks motivated or supported by cybercriminals. The private sector suffers huge financial losses and the population (the ordinary users) becomes victim of cybercriminals in terms of credit card fraud and similar forms of theft as well as unwittingly handing over their private computers to bot herders who set up large bot nets which are involved in several forms of cybercrime in different countries (Anderson; Clayton; Moore 2009). Due to its criminal nature cybercrime is mostly discussed by national security agencies (especially police forces), lawmakers, attorneys, the private sector and government representatives on a national and international level. However, also civil society actors are engaged in the debates on cybercrime. Although they often have different approaches than public or private actors. Besides that, civil society debates about cybercrime often take place in other policy fields of Internet governance, like consumer protection or freedom of speech. Especially the second mentioned is important as it connects the debates on cybercrime with the problem of Internet filtering which will be discussed in the following chapter. Often civil society actors are creating a social balance when actors from the public sector involved in cybercrime debates limit freedom of speech through restrictive legislative processes. In many cases they are also bringing in the necessary knowledge about IT networks which made them indispensable for traditional policy makers.

To understand civil society actors in cybercrime debates (and in Internet governance in general) it needs to be considered that especially in the multi-stakeholder environment of the Internet governance process there is a number of groups and organizations that are not set up as traditional transnational civil society or not-for-profit organizations but who are groups or associations of individuals actively involved in Internet governance without fitting into the classical NGO scheme. One example are the innumerous Computer Emergency Response Teams (CERTs) which exist individually in several countries (often within academic institutions) all over the world and are made up of experts dealing with cybersecurity issues. Another example is the Anti-Phishing Working Group (APWG) which despite of its international placement is also more an association of experts rather than a transnational civil society organization.

In the Internet governance process these non-traditional organizations are on a par with traditional NGOs which differ from non-traditional expert groups by offering a much more complex task structure including agenda setting, fund-raising, public relations and more (Ahmed; Potter 2006 p. 37ff). Furthermore, traditional organizations can be distinguished into those who exclusively concentrate on cybercrime issues (optionally besides other Internet governance topics) and those focusing on problems which due to technical development also became online issues by the time. This means there are (traditional and non-traditional) civil society groups and associations founded with the objective to focus on IT, cybersecurity and cybercrime issues (e.g. INHOPE, APWG, ISOC) and others which at a certain point of time included these issues into their daily routine (e.g. Human Rights Watch, International Consumer Protection and Enforcement Network, ECPAT International).

Most civil society actors entered the cybercrime debates long time after private businesses and especially the public sector had already been dealing with the problem. Looking back at the history of cybercrime it becomes clear that law enforcement agencies and also legislative authorities were much earlier concerned about cybercrime than most parts of civil society were. Exceptions were those individuals and associations involved in the early hacker scene (like IT engineers) who were interested in the Internet more from a technical than from a political point of view. Although the basic philosophy of the early hackers movement also included ethical and political aspects like the urge to create transparency and access to information for everyone. In the middle of the Cold War this demand did not match with the general conception of Western governments. However classical civil society organizations did not start to get involved in the debate on Internet governance and cybercrime until the 1990s when the commercialization of the Internet began. At that time especially IT-oriented organizations like the Internet Society and the Electronic Frontier Foundation (EFF) were the first ones to enter the international (although at that time not yet global) discourse on digital rights without focusing exactly on cybercrime.

During the first decade of the 21st century especially consumer protection organizations and NGOs working on child protection included cybercrime issues into their field of operation. And although the public sector had a certain advantage of working with cybercrime for several decades already, the diversification of both technology and cybercrime lead to a situation in which especially the public sector lost track of certain aspects of cybercrime and not only depended on

civil society experts but also lost reputation (and votes) in several cases where it tried to solve problems relying solely on its own expertise. Examples are the debates on child abuse and Internet filter in several European countries which demonstrated the knowledge gap within the public sector (see next chapter).

Civil society organizations, which undoubtedly are among the winners of the multi-stakeholder approach, used the first mandate of the IGF to prove their competence in several IT issues and influenced especially the public sector's cybercrime policies by delivering quality background information about technological and also social issues. The IGF was a useful forum for these organizations to present their expertise as in most countries outside of the UN context national governments continuously preferred to decide on their own about cybercrime legislation and containment strategies.

Since the beginning of the IGF process civil society has increasingly influenced opinion-making concerning cybercrime in a number of countries. Especially in those countries where civil society has a strong background in the population and can therefore influence voters. In Germany civil society actors called public attention in 2009 during their campaign against a national Internet filter law which the German government developed in their effort to go against criminal acts on the Internet (Krempl 2009b). Constant lobbying for a more effective way to reach the same goal without endangering freedom of speech online lead to a growing support within the population and later forced the government to give up their original plan and to follow the recommendations of civil society actors (more details in the following chapter). This development did not simply generate a short time disgrace regarding the government's (and the opposition's) competence in current IT and cybercrime issues. It furthermore strengthened civil society actors on their path to enter the German public sector within their own political party (founded in 2006). This party, which focused on IT topics only, achieved contrary to the expectations of election analysts 8,9% in the election of the Berlin House of Representatives in September 2011 while at the same time the coalition partner of chancellor Merkel's national government reached 1,8% and therefore did not achieve a single seat in the German capital's House of Representatives (Sueddeutsche.de 2011).

However, although the German case illustrates the growing importance of IT issues and civil society actors in national politics a more in-depth comparison between a number of states is

necessary to analyze the broader scenario. A comprehensive measurement of civil society influence on public policy regarding cybercrime legislation will not be carried out at this point of time but can be the basis for a future research project. Nevertheless, one aspect can already be stated in this context which is the ineffectiveness of single national legislative processes to reduce cybercrime. Even in case civil society had a progressive influence in a limited number of countries it is the global harmonization process that would lead to a containment instead of a restructuring process of this transnational problem. However, global harmonization has proven to be a challenge so far. In this regard, Marco Gercke, director of the German Cybercrime Research Institute pointed out in an interview with the author:

> Harmonisation of Cybercrime legislation can only work to a certain extend. Comparative law analysis in the field of illegal content underline, that the national traditions significantly differ. (...) With regard to the fact that in the last 15 years various countries – especially developed countries - implemented national legislation many of those countries do not see any pressure to harmonise legislation. (Gercke 2011)

Chapter Five: Internet Filtering

When in the 1990s the Internet started spreading step by step all over the world it was seen as an uncontrolled and uncontrollable medium improving and facilitating communication between all parts of society within countries as well as between countries (presupposed they had access to the necessary technologies). The transborder character of the Internet created the impression that governments were about to lose control over the flux of information diminishing especially the power of authoritarian regimes. Therefore the Internet and other information and communication technologies (ICT) were considered a crucial mean to support democratization processes in non-democratic countries.

In the 1990 the spreading of the Internet took place mainly in the USA, Western Europe and Japan. During this first wave of Internet proliferation a focus was given not only on the opportunities new technologies offered to the private economy but also their meaning for citizens to improve their political participation. In an early attempt to explain this potential and its impact on democracy in the United States, Lawrence Grossman developed the idea of an electronic republic in which modern ICT are providing citizens with a wider access to information as well as a growing influence in policy-making processes by exchanging information with other citizens, political organizations or political representatives (Grossman 1996). Research was also conducted on the relation between ICT and government respect for human rights (Richards 2002, p. 161). Although the author of that study did not find any concrete proofs he suggested there may be a positive relation between the two variables (idem, p. 181). Although this vague argument is not sufficient to develop a meaningful conclusion on that question, the author's statement reflects the positive attitude towards ICT and democratization which was characteristic especially for the 1990s:

> A simple empirical test found that although there is no statistically significant direct relationship between a country's level of connectivity and its level of government respect for human rights (…) connectivity may have a very modest indirect role in improving government respect for human rights by aiding democratization. (idem).

There is no doubt that the Internet and other forms of ICT support democratization processes rather than constrain them. Although little can be said so far about successful transition processes from authoritarian to democratic regimes by support of the Internet as there are no cases to be

studied. Even the intensively observed upheavals in North Africa in 2011 did not lead to a democratic transition so far but merely managed to overthrow their totalitarian governments (Asseburg 2011, p. 17). At this point of time it is too early to come to a conclusion regarding the question which way the respective region is going in the next years.

The idea that the Internet would automatically improve democratic processes by empowering citizens and civil society organizations was undoubtedly true for democratic countries in which freedom of expression and political participation were considered also by the elites as fundamental aspects of social stability and development. However, non-democratic countries in the 1990s offered a completely different situation as local elites often considered freedom of speech and political participation as practiced in Western democracies as a threat to their own political and economical interests. For this reason the spreading and application of modern ICT took a different path in non-democratic countries. As will be shown in this chapter, authoritarian regimes were certainly confronted with a new situation when pro-democratic forces started using the Internet, especially during the first decade of the 21st century. Nevertheless, Western technological progress did not only offer the necessary tools to improve political participation, it also consequently developed the anti-tools which supported authoritarian rulers to maintain their political power: the filter software.

Software to filter the Internet was used in the USA already in the 1990s, usually to control content in schools and public libraries. But also home editions were sold to private users in order to prevent children from accessing unwanted websites (e.g. hate speech and adult content). Similar products were developed (mainly by U.S.-American companies) to filter Internet content on a larger scale. As of the end of the 1990s it became clear that these products were used by a number of countries to control Internet content on a national scale. When Saudi Arabia was still waiting for its first Internet Service Provider in October 1998 there were already reports about the government's plans to filter the Internet to prevent citizens from accessing content considered undesired by their government (Gardner 1998). At that time China was already known to filter the Internet (Koppel 1996). Although it took another decade before this topic became a subject of recognized academic research.

In the 1990s, when political and social researchers were focusing on the possibilities the Internet offered to support democratization processes the seriousness of Internet filters was frequently overlooked. Only in the first years of the 21st century awareness was growing and the possibilities of limiting Internet access due to political interests gained more attention, especially because of research institutes like the Berkman Center for Internet and Society (Harvard University) and the Oxford Internet Institute. However, the key event that directed global attention on the possibilities governments could have to control the Internet happened during the so called Saffron Revolution in Myanmar in September 2007.

Myanmar's Saffron Revolution was caused by a disproportionately high increase of fuel prices by the military government on 15 August 2007. Following researchers of the Australian National University prices for diesel, petrol and gas were increased between 160% to 500% leading to smaller protests on which the government reacted with a large number of arrests (Skidmore; Wilson 2008). In the following weeks protesters were joined by a growing number of Buddhist monks until up to 100.000 people participated in the protests. By that time, the focus of the manifestations had already gone beyond the initial fuel problem and included requests for democratic dialogues and the release of political prisoners (idem). The growing numbers of protesters and the growing tensions in the country had drawn international attention on the situation. However, official restrictions inhibited most international journalists to enter the country (RWB 2010). For this reason information about the protests was published by activists in and outside of Myanmar on the Internet. A number of cell phone videos and photos showed protesters marching the streets of the country's largest city and former capital Yangon. Others showed violent confrontations with the police and dead victims among the population. When due to the images of the manifestations international protest was growing the government under General Than Shwe decided to close down the Internet and thereby preventing the circulation of information outside the country. Before that day there was only one similar case in which a national government disconnected a whole country from the Internet which happened in Nepal in February 2005 but which did not attract as much interest as Myanmar did two years later (Waldman 2005). In Myanmar this measure was implemented by temporarily closing down the two Internet Service Providers on 28 September 2011, which were under control of the national government (Skidmore; Wilson 2008). The following day also mobile phone networks were shut down (Chowdhury 2008).

Myanmar's decision to close down the entire Internet was not only a very rigorous one, it also made clear to the international community that although modern ICTs served as tools to support democratization processes, authoritarian governments were about to learn how to control and instrumentalize modern means of communication for their own interests. In this context, the complete disconnection of a country's networks from the rest of the world was not the most common way authoritarian regimes were choosing. The more popular way to control information flows was to install Internet filters. What started as a quite rudimentary way of controlling content in the 1990s became more and more sophisticated in the first decade of the 21st century. In fact, only few years after the Internet was connecting most countries of the world, an ever-growing number of techniques and technologies was in place to impede Internet users from freely accessing any information available online. The following paragraphs will focus on the most common methods used to filter the Internet. After that, the specific singularities of Internet filters in democratic and non-democratic countries will be discussed.

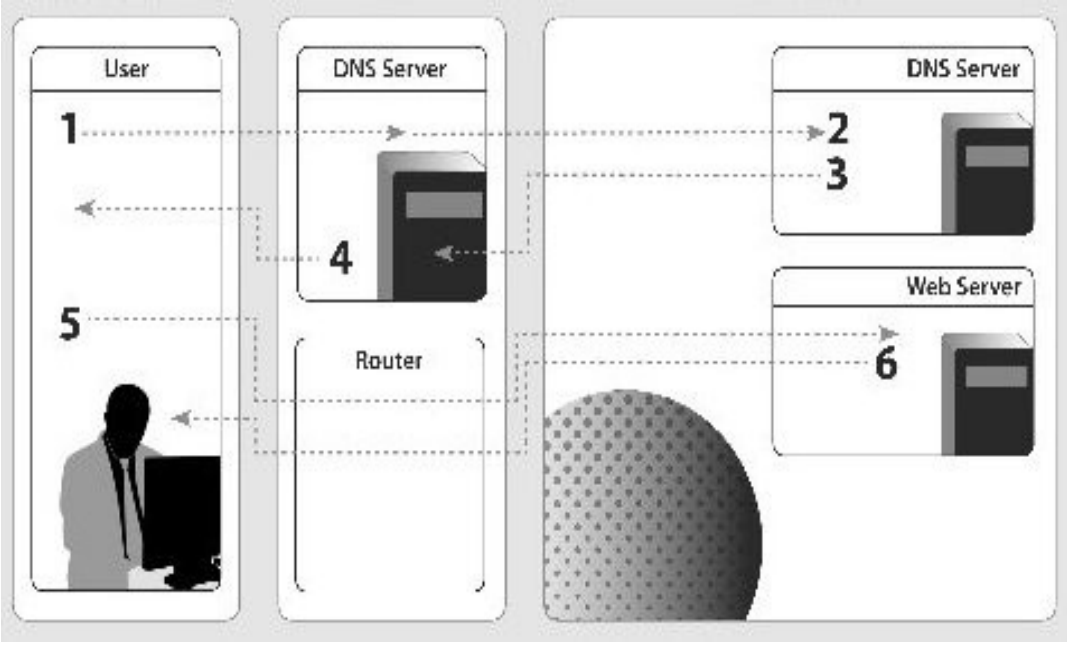
5.1 Methods of Internet Filtering

To understand Internet filtering it is necessary to take a closer look at the technical details of this problem. In interdisciplinary areas like Internet governance it is important to acquire knowledge of different areas of study to be able to fully comprehend the whole picture. A fact, that most traditional policy-makers are still struggling with when it comes to the Internet.

As mentioned before already, information on the Internet is send out in separate packets which are making their way through the global networks to be finally reconnected on their target destination, a computer equipped with its own IP number. To reach this goal a number of hosts (computers) on the network needs to be queried to locate the host the user is trying to connect to (for example a web server on which a website is located). These queries are usually carried out by Internet Service Providers (ISP) which once they spotted the correct web server send its location to the initial enquirer to connect the two hosts. This way the information (e.g. a website) that is stored on one host (e.g. a web server) will appear on the monitor of the user's computer.

As shown in figure 5 this process includes a number of steps before the information is sent to the user. The main task in this process is to translate a web address, also known as a Uniform Resource Locator or URL (e.g. unb.br) to its IP number and then locate the host with that IP number on the Internet. Every computer, host, or web server on the Internet has its own IP number, there is no chance that two machines are having the same number. However, it is possible that a host has more than one IP number. This is the case for example for professional ISPs that are hosting thousands of websites of which each is connected to its own IP number. But also non-commercial servers can have several IP numbers to separate different subdomains. In case of the University of Brasilia the IP number is 164.41.101.33. This number is connected with a server that is located inside the university campus hosting all websites of the university's institutes. All institutes having their own websites within the web server of the university are using a different IP address. This way the Institute for Political Science has a different IP address (164.41.101.34) than the Faculty of Medicine (164.41.147.40) and so on. Including one of these IP numbers into the address line of a browser has the same effect as including the respective URL: it will connect the user with the web server of the university and open the chosen website.

Figure 5: Standard Web-Browsing



Source: Deibert 2008, p. 58

In figure 5 the web server of the university would be on the lower right, marked with position 6. To access the university's web server (and its main website) the user in position 1 would write “www.unb.br“ in his browser which will then be passed on to his service provider that connects him to the Internet. The service provider (in the graphic marked as a DNS server next to the user) will pass on this query to another DNS server in a higher position of the Internet's hierarchy (position 2) and if necessary to a third one (depending on the URL) until the IP number of the web server which is hosting the website unb.br is located. This information will be send back to the user's service provider (arrow 3) and to the user's computer (arrow 4) which will then connect via a router of its service provider with the corresponding web server (position 5). This one will then send back the information (website) to the user's computer (arrow 6). This process usually takes less than a second.

To filter the Internet which means preventing users from accessing information on selected websites an interference needs to take place on one of the different stations seen in figure 5. There are several options to reach this objective and in fact their number is growing over the years due to technological innovations. In the following paragraphs the main types of Internet filtering methods will be presented. At the same time examples will be given how these filters could be applied by the virtual state of Filterland. The idea of this virtual state is to create a scenario which will not only help to explain important aspects of this research project but which will also be useful in the future as a didactical model to instruct Internet filtering in higher education classes of international relations.

In this scenario Filterland is a fictitious state in the early 21st century whose citizens have regular access to the Internet. The country's elites agree that a constant flux of information is a crucial condition for economic development. Therefore they encourage the population to get connected to the Internet to expand economic growth and improve the national level of education.

5.1.1 Method 1: TCP/IP Filtering

TCP/IP filtering can happen in two different ways: header filtering and content filtering (Deibert; Palfrey; Rohozinski; Zittrain 2008, p. 59). In both cases the filter process happens at the router level, which means on position 5 of figure 5. This means steps 1-4 will happen without any limitation. Also in both cases the filter process is based on an analysis of the individual packets sent over the network. This analysis is conducted by the router belonging to the user's service provider. The easier and less cost-intensive of the two ways is header filtering. It uses the standard process of header scanning for IP addresses to find out where the router needs to send the information. If the IP number in a packet's header is blacklisted by the router's ISP the information will be blocked and the query will not be sent to the respective web server. As a consequence the user will not be able to access the website he is looking for. Although it is possible to use several IP numbers for a single server it is also common to use one single IP number for one server on which several websites are stored at the same time. This kind of shared hosting (also known as virtual hosting) is cost-effective but in case of IP filtering the complete server will be blocked. Even though if only one website is supposed to be filtered.

The second way of this method is focusing on the content of the packets instead of the IP address. By scanning not the header but the content of a packet, routers can search for keywords connected to unwanted content. Similar to the scanning for certain IP numbers the discovery of blacklisted keywords will automatically result in a blocking of the query. This more sophisticated way needs additional soft- or hardware as standard routers are not developed to scan for keywords. In case keywords are split up and distributed over more than one packet content scanning will not be successful.

Scanning packet content is also known as deep packet inspection (DPI). While in the 1990s DPI was developed by the IT security industry to scan packets for malware and other security concerns it also became an important issue in the 21st century in debates on Internet censorship (Rhoads; Chao 2009). So far, there is little research done on DPI from a political science or international relations approach. Exceptions are Wagner (2009) and Bendrath (2009). Because of its subliminal character Internet filtering via DPI is likely to increase in the coming years.

Figure 6: TCP/IP Filtering

Scenario 1:

In scenario 1 Filterland is arguing with its neighboring country over a long lasting controversy regarding ethnic minorities in the border region of the two states. For historical reasons both countries are having a significant number of minority groups ethnically belonging to the respective neighboring state (a scenario as it can be found for example in Eastern Europe, Central Asia and the Caucasus region). International human rights organizations have been frequently criticizing both governments for disrespecting basic rights of the minority population. When during an important election year reports about human rights abuse on their own territory intensified, Filterland's government decided to blockade information on that issue to not risk a defeat during the national elections. To reach this goal, Filterland's government decided to manipulate data flow within the ISPs which all belonged to private companies. Due to national telecommunication legislation service providers need to accept government interference without being able to oppose this step.

One year before the national elections Filterland's government handed a list to all ISPs informing them about a number of IP addresses to be blocked. The addresses listed represented a selection of major human rights organizations that had their files stored on servers all over the world for what reason Filterland has no access to the web servers themselves. By using the header filtering method Filterland's ruling party aims at keeping the reports of the respective organizations out of the national discourse on ethnic minorities.

A few weeks after the filter was implemented members of the government still in power realized that by blocking the complete websites of human rights organizations it also became impossible to access information on the situation of minorities ethnically belonging to Filterland but living in its neighboring state. These information served well during the election campaigns to appeal to national sentiments which the current government planed to exploit for its own success. Furthermore, human rights activists mirrored websites of the organizations and their reports which they also published on other websites and blogs which could be found by general search mechanisms on the Internet. To continuously keep

information on human rights abuses in Filterland out of the national discourse, Filterland's government decided to opt for the second (more expensive) way of filtering on the ISP level by listing keywords regarding ethnic minorities on their own national territory. This way reports on discrimination of their own ethnic minority population outside the national borders could be accessed while information criticizing national minority policies were excluded from the national networks.

5.1.2 Method 2: DNS Tampering

As figure 5 shows, the first step of an Internet query is the connection between the user and the provider, displayed as a DNS server in the graphic. During this step the DNS server is initiating the translation from the written URL (unb.br) to the respective IP number (164.41.101.33). To apply the method of DNS tampering the filter software is installed on the DNS server to prevent the translation from letters to numbers. This way, if a computer is sending a query including a domain name which happens to be on a list of blocked websites, the translation process will end at that moment. Without the translation to an IP number the computer will be unable to locate the web server and the process is over. Usually the user trying to connect to the blocked website will receive an error message on his monitor informing about the non-existence of the domain. This process regarding non-existent domains is called NXDOMAIN response (Andrews 1998). Alternatively the institutions or individuals responsible for the filtering process can let users be redirected to a different domain. This so called DNS hijacking process can be used in different manners: 1) to transparently inform users about the filtering process by showing a block page (e.g. Bahrain and United Arab Emirates), and 2) to disguise the filtering process, e.g. Tunisia and Uzbekistan (Deibert; Palfrey; Rohozinski; Zittrain 2008, p. 16). Countries concealing their filtering practice do this by leading users to a forged error page or simply a different website. In other cases users are mislead to a different website in order to abstract data (a process used for example by cybercriminals to steal credit card information or passwords). A further option is not to lead the user to a different server but to simply ignore the query which will automatically lead to an error message (Dornseif 2003).

Figure 7: DNS Tampering

Scenario 2:

In the second scenario Filterland is tending to protect its telecommunication and Internet market against foreign companies that manage to offer their services at better prices. Filterland's policies to develop its national telecommunication and Internet industry includes a number of measures to strengthen among other things the country's online service providers which recently suffered competition from well established international business rivals. Based on its experience of other industries that could not sustain their position due to their global competitors (which caused a notable number of job loss in the country), Filterland's government is eager to not let the same happen to the national service providers. An international market analysis unfolded that a manageable number of global providers (in the following called providers A, B and C) had the capacity to enter the country's market and offer services that because of the size of the companies would outpace Filterland's own service providers. As different to Internet service providers, online service providers do not necessarily need to be physically present in their clients' countries, this problem presented a new challenge for Filterland's economy.

At the same time as Filterland is intending to strengthen its national economy it fears that open restrictions against foreign companies would harm its reputation and thereby its international trade relations. Therefore, the country's government hesitates to openly interfere with foreign providers and decides to subliminally derogate consumers' trust in the respective enterprises. The objective is to reduce service quality of the international providers A, B and C and thus harm their reputation as reliable service companies. This measure would be taken until national service providers had gained a sufficient and stable number of clients and the necessary business experience to compete with its international rivals on the national market.

To succeed with their plan, Filterland's government decides to use DNS tampering as the quantity of IP numbers in question is relatively small. Each of the three companies has

certain IP numbers over which clients get access to the service providers. By activating the filter process on the level of the country's DNS providers, all queries regarding the IP numbers of companies A, B and C are ignored by the providers and end up in an error message on the user's monitor. To avoid international criticism the government decides to use DNS tampering on a temporary basis. This means that the filtering technique is applied in irregular intervals. This way the company is not denied to enter the national market. But in the course of time it will be struggling with discontent clients (unable to access the server whenever they want to) who then might opt for a national service provider where they can access the services they paid for at any time without obstacles.

A similar step of protectionism like in figure 7 was taken by the Chinese government in December 2010 when Internet telephone providers (Voice over IP, VoIP) were declared illegal to protect national state-owned telecommunication companies. Before China already other countries (e.g. Panama) took this step (Leyden 2010). However, international criticism focused on China due to its size and global economical impact, while other cases were mostly ignored.

Already before December 2010, the website of the biggest VoIP provider in the world (Skype) had been filtered in China and redirected to its Chinese partner company TOM Group, where a special version of the software was available. This version was adapted to Chinese laws and regulations and allowed monitoring of conversations and text messages while the original Skype software uses cryptography to protect conversations.

5.1.3 Method 3: HTTP Proxy Filtering

The third among the most common methods of Internet filtering is the integration of HTTP proxy servers. A proxy server functions as an additional instance between the user and the DNS server. In case it is implemented the user will not be able to connect directly to the Internet but will instead access the proxy server which will then send out the query to the respective DNS server. The answer from the DNS and webserver will then be sent to the proxy that is transferring it to the

user's host.

Proxies are used by many Internet providers because they offer certain advantages to reduce costs and speed up connections. For this purpose they need to work as a cache, a memory saving past queries and websites so that in case users want to access a website several times, the provider does not need to send the query to the DNS server each time but can transmit the information stored in the cache. This way users get faster access to websites while at the same time providers can reduce expenditures by limiting bandwidth usage.

Besides improving the user's online performance, HTTP proxies can also be used to filter the content users have access to. This method of filtering shows certain advantages for the filtering actor compared to the previous methods. Proxy filtering can be more exact than IP blocking or DNS tampering as it works on a URL basis and can therefore block individual sites without blocking a complete server or domain (Dornseif 2003, p. 13). In this context there are two types of HTTP proxy servers to distinguish: transparent and nontransparent proxies. While a nontransparent proxy needs a configuration of the browser before the user can access it, a transparent proxy will be accessed by all users without any further configuration on their side. In fact, users often are not aware that a transparent proxy is installed. Different than a caching proxy, filter proxies do not speed up Internet traffic but slow it down. For this reason they can be an expensive tool in case the provider decides to invest in further hardware to adjust the slowdown caused by the proxy (Deibert 2008, p. 63).

In an experiment conducted in the year 2000 students at the Merz Akademie in Stuttgart (Germany) used a proxy server to test Internet filtering on user behavior (Dornseif 2003, p. 13). For this reason they configured a number of university computers in a way that its users were getting Internet access through the proxy. At the same time the proxy was manipulating a number of user activities. For instance it was suggesting personal (fake) pen pals chosen on individual surfing behavior or including advertisement pop-ups on student websites within the university domain. While in 2010 these occurrences were already common for many web services, in the year 2000 the situation was different: the then mostly unknown Internet company Google (which built its later success on a similar model of analysis) was only about to start connecting user behavior with certain results (like advertisements). Besides these relatively hidden manipulations the conductors of the experiment also exchanged a number of words altering the sense of several websites. In this

context “violence“ was exchanged for “love“, the German expression for Middle East (Nahost) was exchanged for Balkans (Balkan), “politics“ was exchanged for “cash“, “censorship“ for “information protection“ and so on.[40] Although the experiment lasted for several months (an exact number is not given), the manipulation went unnoted by the users. Even after it was made public only few users showed concern about the observation of their online behavior and the manipulation of their search results (idem).

Besides the simple form of proxy filtering there is also an advanced measure including TCP/IP filtering techniques. This way a list of IP addresses is used to do a pre-filtering as described in method 1 with the slight difference that queries containing listed IP numbers are not automatically blocked but send to a transparent proxy server. There, a second analysis takes place focusing on the complete web address. While in a DNS tampering process a domain name (e.g. unb.br) will be blocked completely, the proxy will focus on certain URLs (e.g. irel.unb.br/fdhw47de29jdk=2) and leave the rest of the domain unmodified. This way only specific sites will be affected, not complete domains or servers. Another “advantage” of this mixed method is that although it is based on the effective method of proxy filtering not all queries need to be processed by the proxy. Queries directed at IP numbers that are not listed will be conducted without any interference which will reduce expenses. Two countries using a mixed methods approach called Cleanfeed are Canada and the United Kingdom (Bright 2004; Akkad 2006). Also Australia started debating about the implementation of a homonymous system but by 2010 had not yet come to a decision (Welch 2010).

Figure 8: HTTP Proxy Filtering

Scenario 3:

In scenario 3 Filterland's government sees itself confronted with a growing interest of media enterprises being challenged by upcoming business models offered by the Internet. In the decades before the expansion of the Internet a number of large media enterprises was celebrating steady economic growth of their music sections. Parallel to the expansion of the Internet their sale figures decreased as sharing music over computer networks became popular

[40] The complete list of expressions can be accessed at: http://odem.org/static/insert_coin/wordlist.txt.

among music consumers. The traditional business model of the music industry, consisting of sound carriers (usually CDs) live shows and merchandise products, was being challenged by file sharing platforms where users exchanged several kinds of archives, among them music and video files. At the same time as sales numbers were going down a variety of artists discovered computer networks to develop their own business strategy questioning traditional copyright laws. In this context new forms of copyright were presented that adapted to modern forms of digital data exchange. Besides that, artists started developing distribution models that focused less on sales numbers of music carriers and more on live shows.[41]

However, advocates of the music industry decided to defend their traditional business model. By lobbying decision makers and initiating public relations campaigns they influenced Filterland's government to support their request. As a consequence government officials developed a law declaring file sharing services to be illegal by infringing intellectual property rights. National Internet service providers were instructed to delete file sharing services hosted on their own servers and to block selected file sharing websites which were located on servers outside the country. To reach this goal ISPs were forced by law to implement HTTP proxy filters. This way the country did not risk to interfere with general connection speed as all queries were going through a process of IP scanning before those queries including IP numbers referring to known file sharing services were sent to proxies, analyzed and blocked if necessary.

Also this third scenario includes details closely connected to empirical examples. In fact, debates on intellectual property rights intensified since peer-to-peer file sharing became popular at the end of the 1990s (Oram 2001, p. 26). One of the most influential contributions to this debate was the foundation of the Creative Commons non-profit corporation in 2001 by Lawrence Lessig, Professor at Harvard Law School. Together with a team of researchers Lessig presented a set of copyright licenses in 2002 adapted to the challenges of the digital age (Lessig 2004, p. 282). Since then a growing number of publishers and artists used this form of copyright addition to protect their products and outputs while at the same time make them available on the Internet. However, copyright owners continuously tried to influence governments to protect their traditional business

[41] In Brazil researchers of the Getulio Vargas Foundation analyzed a respective case on electronic pop music whose protagonists created a new form of commercialization in which music was distributed for free while at the same time live performances were creating highly lucrative revenues (Lemos et al 2008).

models. In a number of countries this debate resulted in the so called three-strikes model (also known as graduated response model) which intended to completely cut a user's Internet connection for a determined time frame in case he was registered downloading legally protected files. In 2010 among the countries that had already implemented a respective law or were debating its implementation were France, Ireland, New Zealand, South Korea and the United Kingdom. In September 2011, the development of a similar law was also proposed in Germany (Krempl 2011). Although a previous debate in 2009 lead the German government come to the conclusion that the three-strikes model would infringe German privacy laws (Krempl 2009e).

Also individual providers were forced by governments or amicable arrangements with market leaders of the entertainment industry to block access to file sharing servers. Cases of permanent or temporary filtering and blocking are known from Denmark, India, Ireland and others (Chacksfield 2009; Collins 2009; NDTV 2011).

5.2 Internet Filtering in Non-Democratic Countries

When debates on Internet filtering started in the 1990s its main contributions came out of the United States of America. Technological developments in the U.S. not only brought inventions to improve quality and speed of the global network but also methods to control access. The early motives for Internet filtering were based on the wish to prevent children from accessing content that was considered “unpleasant or threatening“ (Rosenberg 2001, p. 35). At the same time the first non-democratic and authoritarian governments started experimenting how to transfer their policies of controlled access to information (or censorship) to the World Wide Web. While on the one hand they saw a number of advantages in using the Internet especially for economical reasons it also represented a new challenge as uncontrolled information flow and easy distribution of any information on a large scale did not mesh with their view of what citizens should be able to see, read or say. As most authoritarian-ruled countries did not belong to those states whose citizens were quickly getting Internet access there was no real pressure on their governments in the 1990s to limit information access online. However, in the course of time Internet filtering regimes became more and more popular and professional in a number of countries.

Most frequently mentioned is the Chinese filtering system, also known as the Great Firewall of China. One of the main reasons for this focus is China's current position in the global economical and political system. While Western countries are struggling with their economical development China is gaining more and more ground not only in Asia but also in other parts of the world. After decades of mistrust during the Cold War, the new global constellations of the 21st century made political analysts in the Western world become frightened again or at least skeptical by their former (and future) opponent's economical success. In 2008, John Ikenberry, Professor at Princeton's Woodrow Wilson School of Public and International Affairs, pointed out in a Foreign Affairs article that "the Western-oriented world order is replaced by one increasingly dominated by the East" (Ikenberry 2008, p. 23). This argument reflects a generally widespread assumption under which observations of China from a Western point of view continue with a certain type of suspicion. These basic conditions need to be considered to understand why also China's Internet filtering system is one of the most criticized. Besides that, it must be mentioned that China has in deed one of the most sophisticated filtering systems and at the same time the highest absolute number of Internet users worldwide.[42]

On the other hand there are examples of other strict filter regimes which would deserve a closer observation but rarely appear in public debates. Two of these examples are Saudia Arabia and Uzbekistan, both countries with high levels of Internet filtering and both countries with strategic importance to Western governments. Both are considered important allies concerning natural resources as well as strategic partners in their respective regions (Cornell 1999, p. 6; Blank 2008, p. 75; Cordesman 2010). Also the 2005 massacre in Andijan (Uzbekistan), which former British ambassador to Uzbekistan Craig Murray compared to the killings on Beijing's Tiananmen Square in 1989, and which lead to an expulsion of international journalists out of Uzbekistan, hardly made the Western public (and only few researchers) take such a close look at freedom of speech and Internet filtering in Uzbekistan as in China (Neef 2006).[43]

[42] Following Internetworldstats.com China had 485 million Internet users in June 2011.

[43] The official number of dead victims of the massacre was indicated by the Uzbek government to be 175, human righs groups reported about a considerably higher number, about 800 or more. As the Uzbek government refused external interference in the case few independent information is available concerning the occurrences. A report on the events, based on eye witnesses and written by Central-Asia expert Shirin Akiner (research fellow of the British Royal Institute of International Affairs and Professor at the University of London) caused controversial debates as Akiner was confirming the low estimates of victims presented by the Uzbek government (Akiner 2005). During this debate Craig Murray blamed Akiner for spreading propaganda in the name of the Uzbek authoritarian regime (Murray 2005). At a later moment Akiner was confronted with similar accusations during a debate at the John Hopkins

In fact, Uzbekistan's constitution includes two articles protecting freedom of expression (art. 29) and forbidding censorship (art. 67). “Freedom of information, however, can be legally restricted to protect the moral values of society, national security, and Uzbekistan's spiritual, cultural and scientific potential.“ (Deibert; Palfrey; Rohozinski; Zittrain 2010, p. 269). The imprecise character of this definition regarding the possibility of reducing freedom of information is part of what researchers of the OpenNet Initiative call the second generation of Internet control (idem, p. 17). By creating a model of three generations of Internet control (table 5) they made clear that China's Great Firewall definitely has a pioneering character among national filter schemes but is also about to be outrivaled by more efficient models which the researchers located in Uzbekistan and other members of the Commonwealth of Independent States (CIS).

Table 5

Trinomial Model of Internet Control	
First generation	Static blocking of Internet content and services. Lists of IP addresses, keywords, domain filtering, in routers, ISP, international gateways (filter before content enters national networks), more of a permanent inflexible character.
Second generation	Information control, create legal and normative environments, creating self-censorship (providers and news papers do self censorship to prevent being prosecuted based on imprecise regulations), DDoS, can be applied punctual/selective in time (flexibility in time, strategic application). Creation of new laws or application of existing laws to cyberspace.
Third generation	Highly sophisticated multidimensional approach: build capabilities to dominate information content instead of blocking information flow. By targeted campaigns information of adversaries, competitors, opposition or others can be outplayed by governmental (counter)information campaigns (or propaganda). Strong content surveillance is necessary.

Source: Deibert; Palfrey; Rohozinski; Zittrain 2010, p. 22ff

The first generation of the trinomial model can be described as a classical model of Internet filtering using mostly the three methods mentioned before. These methods are applied individually or in combination with each other, depending on different factors like general objective of the filtering process and availability of financial resources. Internet filtering in China is a prototype of this first generation. Beijing was among the first governments to establish a comprehensive filtering system and besides that did not just apply it on the ISP level but also at international Internet

University in the U.S. (Jarvik 2005).

gateways, filtering content before it reached national networks. This early model is known for its static or even inflexible character (*install it and leave it*) which partly makes it prone to circumvention using specific online tools which are available (mostly for free) on the Internet (in case those websites are not filtered themselves).

The second generation of Internet control is made up of a more sophisticated model using techniques of the first generation in a more intelligent way. The central idea of this model is to create legal frameworks and regulations based on which the filtering process can occur. This happens by developing new regulations as well as adapting existing ones to the online environment. By creating imprecise legal text leaving plenty of range for proper interpretation, self-censorship is a common result. This way, especially service providers and online publishers tend to hold back critical information to avoid prosecution. Besides that, this model offers a certain flexibility as it can target different servers or websites for a pre-defined period at individual points of time. To disable selected targets DDoS attacks can be added to conventional filtering techniques. One example of a complex legal framework under which second generation control is happening is the Russian regulation SORM-II, an ICT surveillance regulation that was passed in the year 2000 (Deibert; Palfrey; Rohozinski; Zittrain 2008, p. 180). More examples of punctual blocking via DDoS attacks happened during presidential elections in Kyrgyzstan and other countries in the Central-Asian region (idem p. 26).

The third generation of Internet control is characterized by a completely different approach than its predecessors. Instead of inhibiting access to information, authorities tend to use counter-information strategies to influence (or manipulate) the perception of the users regarding specific topics. This means that rather than blocking information flows, governments target at dominating information content by artificially creating big scale campaigns spreading targeted information (or propaganda) in order to “overwhelm, discredit, or demoralize opponents“ (idem p. 27). In this context the question of Internet surveillance plays an important role as actors involved in third generation control mechanisms need to be constantly aware about information being spread by opponents through digital networks. In countries with less Internet penetration this is a relatively manageable task, especially in smaller countries. As soon as larger parts of the population start using the Internet for political reasons this might turn out to be a challenge, the more complicated the larger the country. To build an effective surveillance scenario of the Internet combined with

counter-information units an advanced level of technology and professional workforce is indispensable, combined with a corresponding financial budget. In 2010 some states were already involved in third generation control projects (not only for political but also for economical reasons). But as these techniques are beyond traditional Internet filtering this topic will not be deepened in this study. Further analysis of this phenomenon which is likely to intensify in the coming years can be found in *Internet and Surveillance* (Fuchs, Boersma, Albrechtslund 2011).

5.2.1 China

Although (as mentioned above) China is not the only country conducting Internet filtering a closer look at their practices is indispensable to understand the empirical dimensions of Internet filtering in the early 21st century. It is not only an example for classical filtering practices but also shows tendencies of adapting new forms of content control categorized by ONI researchers as second generation control (and in deed there are even early signs of third generation practices).

In June 2010 official statistics of the Chinese Network Information Center (CNNIC) showed that China had 420 million Internet users making it the largest online nation in the world (CNNIC 2010). This position was reached due to its disproportionately high digital expansion rate. In 2006 the number of Internet users in the country was still 123 million, thus about a third of the current number (CNNIC 2006). At that time the country was still number two after the USA when it comes to absolute user numbers. Comparing the population size of the two countries it is obvious that China will remain in its leading position and given its economical growth rates it will most probably expand the distance to all other countries in the coming years. The rapid increase of Internet users presented an enormous challenge for the Chinese government which was always willing to control information flows in the country and to avoid discussing topics that were regarded harmful for citizens and government. The official term used by the Chinese government is to “harmonize“ Internet content. In Chinese culture the concept of harmony plays an important role. By harmonizing relations to fellow citizens it is believed to create a better life for oneself. Early references to the concept of harmony can be found in Confucius' Doctrine of the Mean.

5.2.1.1 The Great Firewall

China's efforts to filter the Internet basically happen on two levels: the first being the control of Internet traffic coming into the country (usually know as the Great Firewall of China) and the second being the control within the country's own networks (see next chapter on blogs).

The Great Firewall was conceptually developed by the President of Beijings University of Posts and Telecommunications, Fang Binxing (Pierson 2011) and should not be confused with Beijing's Golden Shield Project. The Golden Shield is an extensive strategy of surveillance, including the Internet, but is not limited to it (Walton 2001). The Great Firewall can be seen as a part of this wider strategy with a focus on the Internet. It is located at the international Internet gateways, the connection points between Chinese and international networks. It is made up of a system of keyword filtering, DNS tampering, IP blocking and other techniques, based on Western technologies like Cisco routers for which reason human rights groups frequently criticized the company.

> Activists and human rights organizations have for years charged Cisco and other Western corporations with actively assisting China in developing censorship and surveillance systems. For example, Amnesty International, Human Rights Watch, and Reporters Sans Frontières have consistently highlighted the issues of corporate responsibility and Internet freedom raised by China’s use of Western technologies. These groups allege that Western corporations have facilitated the construction of China’s censorship and surveillance infrastructure, and that they may even be involved in the system’s ongoing maintenance and operations. (ONI 2005, p. 7).

Such business relations of Western companies with the Chinese and other authoritarian regimes are controversial not only for civil society groups but also for the companies involved. Different than for example traditional arms producers that get criticized for exporting (or in fact for producing) their products, IT companies develop products of a pure technological nature whose intention is to build or connect networks. As a great part of the IT engineers did not chose their profession with the awareness that their products will be used to limit freedom of information in non-democratic countries, companies involved in controversial high-tech deals can easily be confronted not only with NGOs but with professionals from their own area, even from within their own companies. This conflict becomes clear in case of Cisco's 12000 series routers which are a

crucial part of Chinas Internet backbone. One of the features of this router is its capability to manage 750.000 filter rules to secure the network against cyberthreats like DoS attacks, worms and other forms of malware. However, as the user is able to define the filtering rules the equipment can easily be programmed not to look for the name of a specific virus, but for the keyword “democracy“.

And in deed, China is using this opportunity to keep websites on certain topics out of its national networks. Among these topics are some that also in a lot of other countries frequently cause controversial debates (being on the Internet or offline), like violence, terrorism, gambling and pornography. Besides that, Beijing considered a lot more content to be unwanted which Wolfgarten (2006) summed up as:

- Any information contradicting the constitution of the People’s Republic of China.
- Any information disclosing state secrets, violating national security, subverting the government or destroying the unity of the country.
- Any information damaging the honor and the interests of the state.
- Any information disturbing social order or undermining social stability.
- Any information spreading or instigating lewdness, pornography, gambling, violence, murder or terror.

However, no specific legislation was developed to regulate Internet content:

> Despite constitutional guarantees of free speech, in practice, there is little legal protection for freedom of expression, with the judiciary closely following party directives in such cases. Although no legislation exists at the national level to clearly regulate online communication and indicate what ICT content is prohibited, a total of 81 administrative regulations involving 29 government agencies were issued between 1993 and 2007 to articulate various controls on content and communication over the Internet. In addition to Internet-specific regulations, vague provisions in the criminal code and state-secrets legislation have been used to imprison citizens for their online activities, including publication of articles criticizing the government or exposing rights abuses, transmission of objectionable email messages, and downloading of censored material from overseas websites. (Freedom House 2009).

To be more specific: human rights issues, debates on the Dalai Lama and Tibet, Falun Gong, Taiwan, Tiananmen, democracy and a number of other issues are frequently censored on the Internet in China due to Cisco's routers. Also critical comments regarding governmental decisions or behavior for example in times of industrial accidents or natural disasters are affected. Several websites are permanently blocked, among them Wikipedia, Youtube, Twitter, CNN, BBC, Human Rights Watch, Amnesty International and more. Technical research on the accessibility of websites in China was conducted by Lowe, Winters and Marcus (2007), ONI (Deibert; Palfrey; Rohozinski; Zittrain 2010), Wolfgarten (2006) and others.

Moreover, online providers like Skype and all national and international search engines have to adapt to national regulations prohibiting for example the display of search results on certain topics. For Western companies this means accepting guidelines stipulated by an authoritarian regime which often leads to intensive criticism in their home countries. One of the most controversial examples is the U.S. company Google which entered the Chinese market in 2005 and offered a censored version of their search engine based on Beijing's specifications. This step caused disaffection by users and civil society organizations in the U.S. and in several other countries what in turn caused Google to participate in the 2008-founded Global Network Initiative, an organization to defend human rights and freedom of speech on the Internet. However, after the company's email service (and especially email accounts of Chinese human rights activists) fell victim to cyber attacks supposedly originating from China, Google decided in March 2010 to remove filtering mechanisms from their search engine and allow an uncensored access to their service (Drummond 2010). This decision was followed by a virtual relocation to Hong Kong before the search engine was finally blocked by Chinese authorities. For Google this step meant a huge loss of profit from the growing Chinese Internet market. On the other hand it removed the flaw from its reputation when opposing Beijing's censorship regime. The winner of this conflict was doubtlessly Baidu, China's leading search engine which already dominated the national market for several years and in 2010 got rid of Google as a (small) potential rival.

5.2.1.2 Blogs

Besides search engines especially web 2.0 applications and providers are confronted with governmental interference as they are offering a variety of options for users to anonymously speak out their opinion. In this context, besides discussion forums the Chinese blogosphere is a frequent target of online censorship. There are no exact numbers about blogs in China but some data give an indication about the general dimension. In 2007 CNNIC declared in a report that at that time China had about 72 million blogs online and around 47 million bloggers (CNNIC 2007). In 2010, the same institution pointed out that the number of blog users has risen up to 231 million users (CNNIC 2010). Although it is not clear if “blog users“ and “bloggers“ (blog writers) are supposed to be the same category, the general numbers make clear that blogs are a widely used application in China. As the number of Internet users is continuously growing in the country, the blogosphere will do as well. The national blogosphere is therefore one of the major challenges for the Chinese government to be controlled. This control refers not only to the content itself but also to user comments. To reach this goal there are both pre-publication and post-publication filtering methods. Pre-publication filtering requires applications installed on the servers of Chinese blog providers which make it technically impossible to publish postings that include banned keywords. This form of filtering is a common way forced upon national providers by governmental instructions (Freedom House 2009). In other cases, post-publication filtering methods are applied resulting in a deletion of individual postings or comments or in some cases the removal of complete blogs (idem). Procedures like this usually happen within 48 hours after publication and require manual interference while pre-publication filtering is usually done by automatic tools. In few cases bloggers have been arrested and sentenced (some of them to imprisonment) because of their postings (RWB 2011, p. 15ff).

While Western debates on Internet filtering in China mostly draw a picture of an impervious system of censorship, the results of a research project published in 2009 show a more detailed scenario (MacKinnon 2009). Therefore, a big part of political postings are not deleted but for different reasons remain online within the Chinese blogosphere. Even postings on very sensitive topics like Falun Gong, Tibet or Tiananmen can be posted on certain providers, albeit a minority of the ones tested. Following MacKinnon, who is the main investigator of the study, a research fellow at the New America Foundation and long standing expert on China and Internet activism, even

humorous comments on Chinese legislation or social injustice were hardly blocked. MacKinnon explained these results of her study by referring to the differences in the Chinese provider landscape. Thus, there is a certain leeway for Chinese blog providers to delete postings or not, based on their own judgment. This means that depending on the interpretation of the responsible administrators sensitive topics can, and in fact are published on a number of providers. During the tests conducted by the investigators, 14 of 15 blog providers allowed between 56% and 99% of the postings containing sensitive topics to be published (idem). None of the postings was deleted by all of the providers at the same time. In order to not endanger the research collaborators working for the providers analyzed, there is no direct information about which provider is responsible for the more rigorous filtering processes. However, it can be assumed that the major providers are among those with more rigid filtering practices while smaller and less known providers have the possibility to follow a more liberal approach.

5.2.1.3 Green Dam Youth Escort

Besides controlling data flow at its virtual borders and content in several web applications, the Chinese government tried to establish an additional Internet filter which was able to interfere at the very early level, being on the computer of the user. By developing a special software called the Green Dam Youth Escort, also known as the Green Dam, Beijing aimed at what institutions in many countries are aiming at: the blocking of certain content even before the query left the computer. This kind of software is in deed comparable to the first generation of Internet filtering software that is applied in the U.S. since the 1990s. At that time public institutions like schools and libraries started using Internet filter software to block adult content amongst others (see later in chapter). Also Beijing announced that its Green Dam software shall be used to protect children from adult and violent content (Faris; Roberts; Wang 2009, p. 8). In 2009, the first edition of the program was presented which was developed by the Chinese company Zhengzhou Jinhui Computer System Engineering together with the Beijing Dazheng Human Language Technology Academy on behalf of the Chinese Ministry of Industry and Information Technology (MIIT). In June the MIIT declared that from 1 July 2009 all computers sold within China (national and imported products) needed to have the Green Dam software pre-installed (Bristow 2009). Institutions like libraries, schools and

others had to keep the program installed while private users were free to delete the software at any time. Furthermore they had the possibility to administrate black and white lists to allow or block additional websites. However, the original list of content that was to be blocked was administrated and updated automatically through the server of the developing company.

This new directive caused disaffection in and outside of China. While civil society actors and Western governments criticized Beijing for introducing a new instrument of online censorship and for violating free trade agreements, Western IT companies declared to be unable to fulfill the new directive within the short time given. Also Chinese retail sellers were confronted with the problem of how to deal with their stocks that included a high number of computers without the Green Dam software (Wines 2009; Watts, Branigan 2009). Due to the difficulties to realize the project, the Chinese government decided one day before the official launch of Green Dam to postpone the project. Few weeks later, in August 2009, China's industry and technology minister Li Yizhong declared that the government had refrained from their directive to install the software on private computers (Back 2009). Five months after the project had been abandoned, the U.S. IT company Solid Oak Software sued the Chinese government and the developers of the Green Dam software as well as a number of computer producing companies that had installed the program on their own products. The reason for the charge were 3000 lines of code that the developers had supposedly copied from a Solid Oak filtering software (United States District Court 2010).

While Chinese officials had constantly declared that the objective of Green Dam was to filter adult and violent content to protect children on the Internet, researchers at the Computer Science and Engineering Division at the University of Michigan succeeded to prove that the program was in fact filtering more content than Beijing had pretended (Wolchok; Yao; Halderman 2009). Besides image and URL filters the scientists detected a third mechanism based on keyword and text filters. By decrypting a number of files of the program they found out, that additionally to adult and violent content also political topics were on the blocklist, mostly referring to Falun Gong. Decrypted files of their research on text filtering can be found under the URLs:

https://jhalderm.com/pub/gd/data/xwordl.php
https://jhalderm.com/pub/gd/data/xwordm.php
https://jhalderm.com/pub/gd/data/xwordh.php

https://jhalderm.com/pub/gd/data/falunword.php

Figure 9: Green Dam Screenshot

Source: Wolchok; Yao; Halderman 2009

When translating the content of the files from Chinese to English a number of expressions can be found including “Falun Gong“, “Falun Dafa“ (alternative name for Falun Gong), “Li Hongzhi“ (founder of Falun Gong), “human rights“, “Tiananmen massacre“, “Buddha“ and “Taiwan independence“. Furthermore can be found “Shanghai Gang“ (pejorative expression for a network of influential Chinese politicians related to former Chinese President Jiang Zemin, also known as the Shanghai Clique) and “global public trial Jiang Zemin“. The latter refers to Falun Gong's effort in 2002 to sue former President Jiang Zemin in several countries for genocide against the Chinese people. Jiang Zemin, who as President ordered the prohibition of Falun Gong in 1999, was also subject of a number of symbolic “global public trials“ held by Falun Gong in several countries in 2003 and 2004.

5.2.1.4 Circumvention Methods

When looking at Western debates on Internet filtering in authoritarian countries it is often suggested that citizens are generally not aware of their government's censorship measures or they fear consequences in case of protest and do not know how to help themselves in that situation. In fact, the picture is more differentiated. What is rarely shown is that Chinese Internet users know how to get around filtering systems like the Great Firewall. Common circumvention tools are Virtual Private Networks (VPN) or anonymity tools like The Onion Router (TOR), an open source project originally developed by a group of researcher in the U.S. TOR was presented in 2004 during an IT security congress in San Diego and can be downloaded and installed for free on any operating system (Dingledine; Syverson; Mathewson 2004). Also VPNs are available for free on the Internet although paid versions claim to be safer and more stable. Both VPNs and TOR use file encryption technologies and direct the users to a network of servers providing them with a different IP number than their own host. This way not only average school kids in Brazil, Argentina, France, South Africa and several other countries succeed to access their favorite websites from their school or library networks but also Chinese Internet users manage to bypass the most complex national Internet filtering system in the world. Another interesting indicator for this development is the increase of Chinese Facebook profiles since the company's CEO Mark Zuckerberg visited the country in 2010. Although the website is blocked in China since 2009, the user numbers more than doubled after Zuckerberg's visit (Lococo; Lee; MacMillan 2011). However it is important to mention that bypassing the Great Firewall requires a respective knowledge or assistance by a capable person and a certain knowledge of English language. For this reason it is very likely that only a limited number of people is aware of these options, although the technical means are freely available.

5.2.1.5 International Impact of Chinese Internet Filters

While shortly after the turn of the millennium DNS tampering happened only within national borders this scenario changed over the years. In 2010 a report of the U.S.-China Economic and Security Review Commission stated and also IT security analysts found out that DNS

tampering within Chinese DNS servers was starting to affect queries from other countries as well:

> In March 2010, reports surfaced that China's Internet censorship regime (…) temporarily affected Internet users outside of China. Specifically, certain users in Chile and the United States who tried to access popular social media sites, including Twitter, YouTube, and Facebook, were denied access by being redirected to incorrect or nonexistent servers. (USCC 2010, p. 241).

The reason for this problem was the growing influence of Chinese DNS servers outside of China. IT security analyst Earl Zmijewski, Vice President of IT intelligence company Renesys explained:

> DNS routing is not based on the physical proximity of the Web surfer to the DNS server, but on the business relationships between the firms hosting the root servers and those providing the Web surfer with Internet access. (Roberts 2010).

For this reason, web queries from Chile were directed to a China-based DNS root server run by the Swedish company Netnod, where they were then treated like internal Chinese web traffic which included blocking certain websites. The increasing importance of China's telecommunication industry will intensify this problem. Especially in Asia and Oceania Chinese telecommunication industry is likely to expand in the coming decades. However, on a global market also other parts of the world can be affected as the before mentioned example made clear.

5.2.2 Post-Filtering Surveillance Strategies

It is hardly imaginable that on the long run a complete control of cyberspace will be possible. Just as the racing duel between malware and security software it is always a question of time which party is spotting the latest security hole first. The same goes out to actors interested in filtering the Internet. The Chinese government invested extensive resources to develop an online control system capable of excluding all information Beijing would not want its citizen to access. Nevertheless, the constant changes and innovations of network technologies always open a new window through which users can reach out and get whatever information they are looking for. Just

as Deibert and Rohozinski suggested in their Internet control model (table 5, p. 149), also China, willing to adapt to constant changes in cyberspace, started to include new methods to not simply block content but to influence the quality of information within its own networks.

Part of this strategy is an all-embracing surveillance of cyberspace which especially in case of China is a challenge due to its size and growth rates. In 2010 only a small part of the population (about 36%) had access to the Internet. And this small part is already forming the biggest national user community in the world. Given that the country will keep on growing including the number of people going online, the challenge of watching their online behavior will get even bigger. And getting bigger means requiring higher budgets and more professional work force. “China has demonstrated to many countries that they can try to censor the Internet, but it has also made it clear how massive the financial, labor and operational resources are needed to do so.” (Mueller 2011).

One important question is which path Beijing will chose to expand its control methods beyond classical filtering. As seen before, there are strong evidence that the first steps are already taken by breaking into mailboxes as happened with users of Google's mail service. Other pointers are wider surveillance networks like GhostNet. In both cases there is no clear proof that the Chinese government was directly involved. However, Beijing's offline methods towards its critics suggest that the involvement in cyber attacks is not unlikely. Another possibility is outsourcing cyber control to loyal online citizens. This way Beijing could use the large number of patriotic Internet users who could participate in the surveillance process and contribute to an online environment in which critical voices disappear among a larger number of pro-government contributions. This way, Beijing could avoid being exposed online regarding certain topics, especially in web 2.0 environments where users can easily voice their opinion.

First steps are already taken to realize a consolidated involvement of online pro-government users. Since 2005 a growing number of patriotic users has been observed to contribute with pro-government postings in several online debates in forums and other sites on the Internet (Cook 2011). Referring to the payment they are supposed to receive per posting, they are called 50-cent army or 50-cent party where 50-cent is referring to 50 Chinese fen (5 mao; 0,5 RMB). The origin of these patriotic web activists, also known as red vests, red vanguard or WuMaoDang, goes back to institutional changes in Chinese universities in the year 2005. At that time, Beijing decided to close

down a number of Bulletin Board Systems (BBS) at several universities to avoid uncontrolled online discussions in academic institutions. For this reason a new strategy was developed at Nanjing University that included the forming of a group of web commentators made up of students of the same institution (Bandurski 2008). The strategy of hiring online supporters to create favorable postings in strategic places on the Internet is not a Chinese invention. It is quite common especially in marketing campaigns aiming at the promotion of a chosen product or website (Streitfeld 2011). Although it is highly disputed especially for ethical reasons. The system is simple: Internet users are hired by companies to improve their product's reputation by posting fake reviews on main e-commerce websites or by composing positive clients' comments on a service website. However, the Nanjing web commentators were not chosen to support a product but the Chinese official point of view on a number of issues. The function of these commentators was to follow discussions on the online board and to participate in the debates with pro-government postings. This way critical opinions could be outnumbered and outplayed. By trying to dominate online discussions these web commentators were setting new standards of cyberspace control. While simply deleting unwanted postings could strengthen displeasure of Internet users because of obvious censorship methods, the interference with pro-government comments could create an impression of free speech and at the same time socially exclude or intimidate critical commentators by overwhelming them with a high quantity of patriotic postings.

Due to the success of the Nanjing strategy the same system was then adopted by leading members of the Communist Party who decided to apply it on the national level. In January 2007 China's president Hu Jintao publicly declared the importance of dominating online public opinion. He also made clear that a certain form of “online guidance“ was needed to not just use but also to control the Internet (Bandurski 2008). To realize this plan a large number of people was hired to “guide public opinion“ on the Internet. These web commentators were prepared in special courses by the Ministry of Culture (idem). There are no official numbers but estimates say that in 2008 there were about 300.000 web commentators working for the Chinese government (Fareed 2008). Besides them, a large number of web commentators was hired by private companies to improve the reputation of their products.

Although since 2008 Western media quite often mentioned the 50-cent army in their publications, its existence remained officially unconfirmed. Only in 2010 the English online version

of the Chinese tabloid newspaper Global Times (which is connected to the Communist Party of China) published an article in which the author referred to the 50-cent army. Without confirming the existence of a large number of online commentators as stated in Western media, the paper mentioned the recruiting process of 650 web commentators by a regional government, to “guide public opinion“ on the Internet (Zhang 2010). One year later, in May 2011, also the English version of the People's Daily, a newspaper connected to the Central Committee of the Communist Party of China, brought its first article on the 50-cent army. Similar to the Global Times, the author did not confirm the formation of such a group but built her argumentation on its existence. However, in her column she did not focus on WuMaoDang but on WuMeifenDang, which she presented as a 50-cent party financed by Western powers to discredit China on the Internet (Li 2011). Furthermore she described both as new and popular terms in the Internet age that were causing international discussion. However, in October 2011 online search results of both terms (in Latin script) showed a different picture regarding the international popularity of the two terms. While hundreds of websites referred to WuMaoDang, WuMeifenDang was only found on nine website, all of which had published the same article of the People's Daily.

5.2.2.1 Internationalized Domain Names

When the Internet was developed, the DNS system, which would translate domain names into IP numbers, was based on the Roman alphabet. It was also based on the American Standard Code for Information Interchange (ASCII) which served as a pool from which a number of symbols was allowed to be used to create domain names. These were the letters A-Z, a-z and the numbers 0-9 plus the hyphen. With the growing internationalization of the World Wide Web appeared an increasing need of adapting the old system to the new reality. A variety of countries became interested in using letters from their own languages that were not part of the ASCII (Mueller 2002, p. 224). Some of them differed only slightly as they were based on the Roman alphabet as well. Examples are Portuguese (e.g. ç and ã), Spanish (e.g. ñ and í) and German (e.g. ä and ö). For others it meant being able to use their own languages and scripts as domain names for the first time. Among them were China, Russia, Iran, Greece, Saudi-Arabia and many others. In some cases, such as India, a multitude of scripts within the same country was waiting to be included into the DNS. In

March 2003 RFC 3490 was issued to present the Internationalizing Domain Names in Applications (IDNA) standard which would be responsible for converting non-ASCII-based domain names (Unicode domain names) into ASCII standard (Faltstrom; Hoffman 2003). In the following years several national registries introduced Internationalized Domain Names (IDN) as second-level domains. To avoid a complete reformulation of the DNS the transformation of IDN was happening on the client-side. For this reason respective functions were included into browsers, email clients and other user programs. By means of the punycode standard (which was introduced in RFC 3492 in March 2003) non-ASCII-based domain names were converted into ASCII-Compatible-Encoding strings, so called ACE strings (Costello 2003). ACE-strings are transformed domain names which contain only ASCII characters. This way the domain name relações-internacionais.com.br would be transformed to the ACE-string xn—relaes-internacionais-43b63a.com.br which (based on ASCII) could be processed by the DNS.

In the first years after IDN was introduced it was not very successful as it referred only to second-level domains while top-level domains remained within the ASCII system. Especially for users of non-Latin alphabets this meant using two types of scripts within one domain name (e.g. президент.ru). This required switching the system's language option during the writing process, a cumbersome practice if carried out frequently. To improve and in fact complete the IDN system, ICANN started introducing the first IDN ccTLDs in January 2010, being Egypt, Russia, Saudi Arabia and the United Arab Emirates (ICANN 2010a). All of these requesters had to go through ICANN's IDN ccTLD Fast Track Process which since November 2009 coordinated the implementation of IDN ccTLDs based on a specific implementation plan[44] (ICANN 2009). In June 2010 China's application was approved as well and two Chinese IDN ccTLDs were included into the DNS, one in simplified Chinese (中国) and one in traditional Chinese (中國) (ICANN 2010b). From that moment Chinese domain names including national TLDs could be registered based on Chinese characters and administrated by the DNS. Web queries were therefore transformed into ACE-strings which were readable by the ASCII based root server system. This means, for example, that CNNIC's website is now available under cnnic.cn as well as under 中国互联网络信息中心.中国, which will then be transformed to the ACE-strings xn—fiqa61au8b7zsevnm8ak20mc4a87e.xn--fiqs8s.

[44] *The Final Implementation Plan for IDN ccTLD Fast Track Process* includes the criteria which need to be fulfilled by the requesting country to receive one or more IDN ccTLDs. Concerning the ongoing debate on democratization of ICANN it is important to mention that the last criteria that has to be met by any country is the approval of the U.S. Department of Commerce due to its contract with IANA.

Besides China and the before mentioned, a number of other countries had their IDN ccTLDs included in the DNS, among them Egypt, Morocco, Syria and Serbia. Different than IDN second-level domains the IDN ccTLDs became very successful. For example, in less than two years over 800.000 domains were registered under Russia's IDN ccTLD. Also China had little success in the beginning with the implementation of IDN second-level domain names. In 2000 CNNIC decided to offer IDN domains for free for the period of twelve months. Although over one million domains were registered within one year, this first wave ended in 2003 already. As the early system was quite unstable, many domains were not renewed and the number of IDN domains decreased. To improve the situation of IDN in China CNNIC began promoting the implementation of IDN ccTLDs and decided to go a special way to make pressure on ICANN by starting to operate its own IDN ccTLDs in 2006 already, four years before ICANN approved its inclusion into the DNS (Ward 2006).

To be able to run its own IDN ccTLDs without the IANA root (which was under control of ICANN and the U.S. government), Beijing decided to set up its own root server just for its IDN ccTLDs. A crucial step, as the stability of a globally functioning Internet depends on the stability and the singularity of the root server system. The seriousness of this problem becomes clear when looking back at Jon Postel's root server redirection in 1998 which immediately caught the attention of the U.S. government fearing a manipulation or even a break of the DNS. Wolfgang Kleinwächter was participating in respective ICANN meetings at the time Beijing had activated its own root system, and furthermore he discussed the issue with members of CNNIC and the Taiwan Network Information Center (TWNIC). In an informal conversation with the author, Kleinwächter confirmed that Beijing had established its own root server as a pilot project in 2006. Following his information, this step was taken to strongly underline China's demand to include the countries two IDN ccTLDs into the IANA root. Following Kleinwächter, debates on the implementation of both simplified and traditional Chinese IDN ccTLDs were tense, reflecting friction between Mainland China on the one side and Hong Kong and Taiwan on the other side. The latter two are using mainly traditional Chinese while in Mainland China a big part of the population is using simplified Chinese which was introduced in the 1950 to reduce illiteracy. To solve this conflict ICANN decided to include both IDN ccTLDs into the IANA root in 2010.

For China the introduction of IDN ccTLDs had a number of advantages. Similar to all countries whose languages are not based on the Roman alphabet, also China suffered from the dependency on the English language and the respective alphabet to use the Internet. Although the percentage of Chinese citizens speaking English is increasing, the majority (especially in rural areas) does not speak nor read any Western language. Besides the problem of digital exclusion due to socio-economical factors, the language barrier additionally complicated Beijing's plan to bring a bigger part of its population online. The introduction of both domain names and ccTLDs written in Chinese characters support digital inclusion and foster the development of a national e-commerce infrastructure (Ward 2006). Besides that, the utilization of national languages creates a stronger identification with the Internet and facilitates navigating and searching online for specific information. As most users prefer search terms in their own language, there is a necessity for search results to be in that same language as well. Another important aspect is the existence of more than 40 million Chinese living outside of China. Beijing is hoping to fortify the country's relations to those citizens by using their common language on the Internet. This is also a strong argument why Beijing could not be interested in maintaining its own root server system within the country. A national root system would exclude users outside the country to access websites based on Chinese IDN ccTLDs. Besides that, as Bill Drake put it: "...running something parallel would be pricey and might be an abysmal failure." (Drake 2011). For this reason the inclusion of these TLDs into the IANA DNS was of high interest for Beijing. Also Kleinwächter confirms that China has no interest in cutting off its networks from the global Internet:

> For the moment I see a double strategy in China. They accept the international system as it has been developed as a fact of history but they have reserved their right (in the Tunis Commitment of WSIS) to have full sovereignty over their own domain name space (ccTLD). This allows them to have different policies nationally and globally. (Kleinwächter 2011).

While countries with non-Roman alphabets undoubtedly profit a lot from ICANN's Fast Track Process to include IDN ccTLDs, Western observers showed concern about this development. As many of the countries applying for IDN ccTLDs are known to filter the Internet and to constrict freedom of speech within their countries critics noted they could use their new TLDs to intensify this development. Table 6 shows all 22 IDN ccTLD applicants until December 2010. All had passed the application process or were in its last stadium. Only two (9%) of them did not show any evidence of filtering during research conducted by the ONI. 15 (68%) of them were involved in

Internet filtering (at a low, medium or high level) while in 5 cases (23%) there was no data available (Figure 10). The U.S.-American NGO Freedom House considered 14 (64%) of them to have had no free press in 2010 (Figure 11). Another 5 (23%) were considered to have had a partly free press. This means, that 87% of the applicants for IDN ccTLDs were considered to have had no effectively free press and 68% of them were actively engaging in Internet filtering.

Table 6

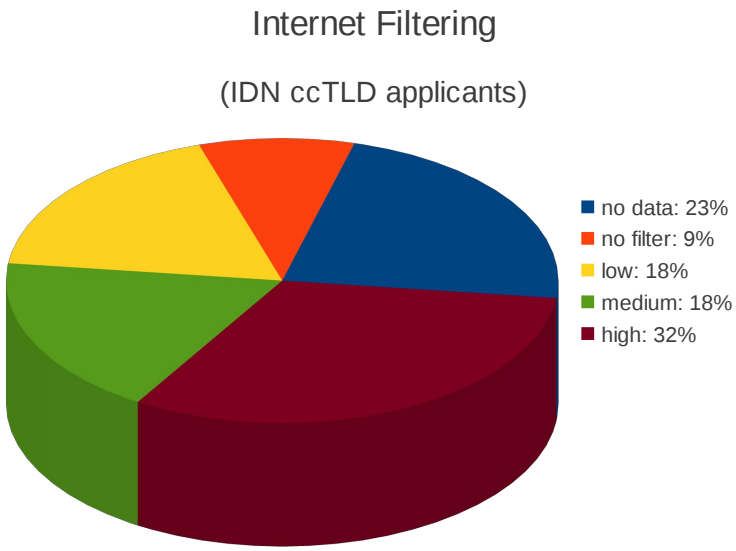
Applications for IDN ccTLDs

Land	Filter Intensity[45]	IDN ccTLDs	Press Freedom 2010
Algeria	no filtering	لجزائ	not free
China	high	中国 ; 中國	not free
Egypt	no filtering	مصر	partly free
Hong Kong	no data	香港	partly free
India	low	भारत ; பாரத ; ભારત ; ভারত ; ଭାରତ ; இந்தியா	partly free
Iran	high	ایران	not free
Jordan	low	الاردن	not free
South Korea	medium	한국	free
Morocco	medium	المغرب	not free
Oman	medium	عمان	not free
Palestine	no data	فلسطين	no data
Qatar	high	قطر	not free
Russia	low	рф	not free
Saudi Arabia	high	السعودية	not free
Serbia	no data	срб	partly free
Singapore	low	新加坡 ; சிங்கப்பூர்	not free
Sri Lanka	no data	ලංකා ; இலங்கை	not free
Syria	high	سورية	not free
Taiwan	no data	台灣 ; 台湾	free
Thailand	medium	ไทย	partly free
Tunisia	high	تونس	not free
United Arab Emirates	high	امارات	not free

Sources: ONI, ICANN, Freedom House

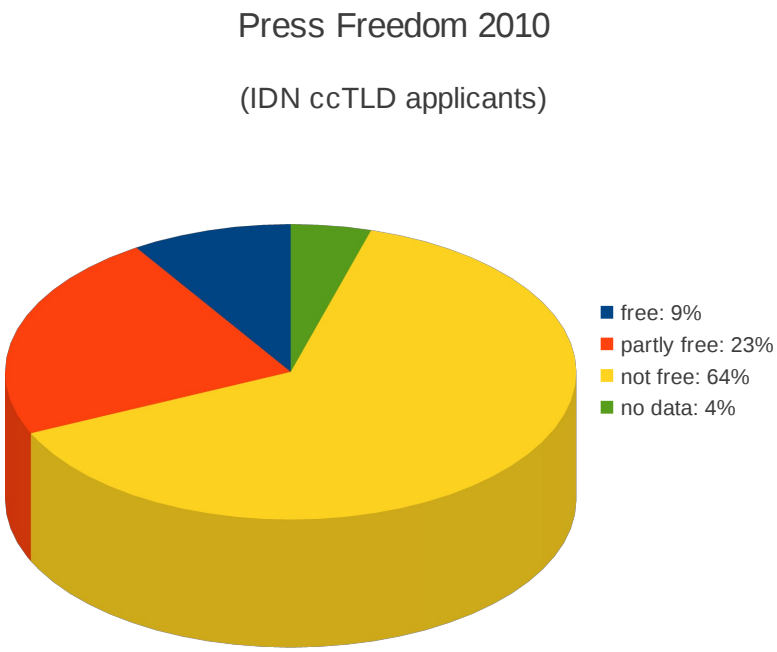
[45] Based on the latest ONI data published in 2010.

Figure 10: Internet Filtering and IDN ccTLDs



Sources: ICANN, ONI

Figure 11: Press Freedom and IDN ccTLDs



Sources: ICANN, Freedom House

In this context the fragmentation of the Internet became an important topic. Within the debate on individual languages nationalistic tendencies were highlighted which could turn the international network into a sphere of national networks that were more focused on their internal interests and content rather than on information coming from outside the country (Mueller; Raad 2008). Critics fear that this development could not only endanger the idea of a global network but could be used by authoritarian governments to enforce their filtering and control regimes. In fact, a national network is much easier to control than a global network in which users access servers from all over the world what in certain cases makes them more independent from restrictive national information policies. The focusing on national content only, could facilitate the implementation of policies complicating the access to foreign providers, for example by special taxation of foreign TLDs. As described before in filter scenario two, measures of protectionism can easily result in soft versions of censorship when it comes to a limitation of access of certain resources (in this case foreign TLDs). A regulated preference of national TLDs combined with a restrictive policy towards foreign content providers will lead to a concentration of users on national content providers which will be situated within the country's own legislation and can therefore be easier controlled than content providers outside the country. Especially in countries with a low level of freedom of speech the restriction of access to foreign providers will pose e serious problem to opposition groups. In countries with a high number of users and a well developed Internet based on IDN ccTLDs, the worst case scenario could be a partly or complete blockade of foreign TLDs making it impossible to access information coming from outside the country. These blockades can also have a temporary character applied at strategic moments like elections, social or political conflicts and more. Another scenario could be the classification of users that will have access to foreign websites by receiving special access codes or passwords (Knight 2008). This scenario can be discussed within the context of net neutrality[46] (Cheng; Bandyopadhyay; Guo 2008).

When discussing Internet filtering in authoritarian countries China has the function of being an example for a highly sophisticated filter regime and at the same time delivering a theoretical scenario about what methods are applied in a large number of other countries as well, even though in a less consolidated package.[47] While debates on Internet filtering have happened since the 1990s the focus has mostly been on states outside the Western world (with few exceptions like the U.S.

[46] Net neutrality is a highly debated topic among Internet governance actors, dealing with the classification of access, speed and other aspects.

[47] For an overview of Internet filtering in a major number of countries see Deibert; Palfrey; Rohozinski, Zittrain 2010, p. 109ff.

library filter debate). Only years later (during the first decade of the 21st century) researchers started to focus also on filtering tendencies in democratic states, especially in Europe, North America and Australia. The following chapter will focus on a debate whose actors are considered by Freedom House to be free of censorship. However, in certain situations their policy plans and choice of expressions do not necessarily differ a lot from those discussed so far, as Kleinwächter made clear:

> However a lot of democratic governments which feel not so comfortable with their limited role in Internet Governance, will do indirectly the same what China is doing. It is not easy to explain to an outsider what the difference is between a "civilized Internet", proposed by Mr. Sarkozy or a "healthy Internet", proposed by the Chinese president. Who decides what civilized or healthy is? A committee? A Politburo? A political commissioner? A court? Difficult. (Kleinwächter 2011).

5.3 Internet Filtering in Democratic Countries

When comparing the quantity of academic studies on Internet filtering it becomes obvious that among the few studies that exist at all, the vast majority is concentrating on the situation of authoritarian states. This is due to the fact that the concept of Internet filtering was mostly defined in Western countries which were highly interested in analyzing classical forms of censorship being limitations of freedom of the press, freedom of speech and freedom of expression in general. At the same time the practice of Internet filtering in their own countries was hardly seen as a serious issue as it was less extensive and was supposed to happen within clearly defined legal frameworks and within a certain level of transparency. Western democratic governments tend to consider Internet filtering in their own countries as their sovereign right to defend democracy while Internet filtering in non-democratic countries is considered a threat to democracy. The first cases of Internet filtering happened mostly in libraries and public schools in the U.S. to block a variety of websites that were considered inappropriate in public spaces where minors were present (Bastian 1997). Blocked websites could contain pornographic material, hate speech and racism, violence and more. During the 1990s a number of public institutions in the U.S. started installing filter software on their computers, including those for public user access. In the year 2000, the Children's Internet Protection Act (CIPA) was signed requiring public schools and libraries to install filter software on all of their computers in order to receive public funding (Schwartz 2001). As a consequence all U.S.

federal states developed individual laws concerning Internet content in public places. The National Conference of State Legislatures offers a complete list of U.S. Internet filtering laws concerning schools and libraries on their website.[48] In the year 2003 the United States Supreme Court declared CIPA to be constitutional.

The problem of Internet filtering software developed by American companies in those days was its inaccuracy due to keyword filtering mechanisms, also known as underinclusiveness and overinclusiveness (Hunter 2000). A problem that in deed continued during the years and until today makes keyword filtering an unreliable measure. As keyword filters search objectively for expressions but cannot analyze the context there is a good chance that websites are blocked just because they contain certain expressions although their actual content does not apply to content that the filter was installed for. A study conducted by the Kaiser Family Foundation, an organization focusing on health policy research, revealed that a variety of Internet filter software products including market leaders as Symantec, Websense and CyberPatrol suffered from overinclusiveness and blocked health related websites like childrenwithdiabetes.com, femalehealth.com, gayhealth.com, plannedparenthood.org, ec.princeton.edu and others (Resnick; Richardson; Hanson 2002). Due to the First Amendment of the United States Constitution which emphasizes freedom of speech,[49] Internet filters in public institutions have become the object of several law cases in the U.S. Examples are the cases Mainstream Loudoun v. Board of Trustees of the Loudoun County Public Library[50] in 1998 (concerning research on breast cancer) and Melvin Urofsky et al v. George Allen[51] in 1998 (concerning research on gender roles).

Also outside the U.S. democratic governments started identifying Internet filtering as a possible measure to control the access to content that outside cyberspace was considered to be illegal as well. In the first 20 years of the Internet the most disputed topics in democratic countries were child pornography and the infringement of intellectual property rights. Other topics that belong to the debate are online gambling, hate speech and national socialist content. In this context various interests and expertises from a variety of stakeholder groups met to find solutions for the respective questions.

[48] The information can be accessed at: http://www.ncsl.org/default.aspx?tabid=13491.

[49] The wording of the First Amandement is: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

[50] Access at: https://www2.bc.edu/~herbeck/cyberlaw.mainstream.html

[51] Access at: http://www.loundy.com/CASES/Urofsky_v_Allen.html

One of the main challenges when it comes to the question of controlling online content is the diversity of legal definitions combined with the transborder character of computer networks (Svantesson 2010). Outside of cyberspace the publication of information or media is regulated by a legislation geographically framed by the national borders of a state in which the publication is available. In cyberspace these borders do not exist. Content that is legally protected in one country can easily be accessed by users in other countries whose legislations do not permit the production, possession or distribution of the same material or content. One example is the distribution of symbols or propaganda supporting national socialism which for example in Germany does not fall under the protection of freedom of speech. For this reason German individuals or groups willing to distribute such material tend to use servers in Canada, Sweden or in the U.S. where freedom of speech is defined in a much broader way. However, hardly any debate has taken place so far in Germany about blocking national socialist content. One exception is the case of the German state (Bundesland) of North Rhine-Westphalia (NRW) which in 2002 tried to establish regulations to block a selected quantity of websites from U.S. American providers containing national socialist content (Krempl 2002). Although this regional filtering model could not be established on the long run, it is considered a first step towards the conflict on Internet filtering that the country would see a few years later. Furthermore, the NRW case also gave a first idea about the general conflict lines which can be found regularly within Internet filtering debates in democratic countries. Similar to the German 2009 debate (which will be discussed later in this chapter), also the 2002 NRW debate was marked by political interests of the public sector in contrast to mainly technical and social interests by the private sector and civil society. The latter two were represented by service providers, the Chaos Computer Club (CCC; a hacker organization advocating privacy rights and data protection) and the data privacy organization FoeBuD.[52]

[52] FoeBuD is the German abbreviation for *Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.*, meaning Association for the support of moving and stagnant public data traffic.

5.3.1 Child Pornography

The discussion on child pornography (CP) on the Internet is happening under different circumstances than most other debates on content regulation. One important reason for this is the fact that unlike extreme political opinions or gambling, CP is not protected by any legislation in the world. Although there are slight differences between a number of legal systems regarding this problem, none of them is offering a save haven for providers distribution respective material. Due to this international consensus there was never a debate *if* states should become active against the production and distribution of CP but *how* they should proceed. Nevertheless, the debate on the procedure also lead to intensive conflicts related to the questions of freedom of speech and freedom of information. Not regarding the right to access the material in question but regarding the questions 1) if the introduction of filtering regimes does not interfere with basic civil rights and 2) if there are more effective measures than filtering to reach the same goal.

Scandinavian countries were among the first in Europe developing filter regimes with the ambition to go against CP on the Internet. Norway started the first initiative in 2004 using DNS-blocking and stop servers like it was suggested by the British Internet Watch Foundation (IWF) at that time (Stol et al 2009, p. 251). The Norwegian blocklist contained about 8000 URLs and 18.000 hits were blocked every day. Interesting to mention is that not all ISPs in Norway were participating in the filter regime. Later also Sweden, Denmark, and Finland started using filters to block access to CP. After the Scandinavian countries also the Netherlands, Switzerland and Italy installed a similar system (idem; KOBIK 2009, p. 14). And also New Zealand, Canada and the U.S. applied filter systems to block CP. While most of the countries mentioned developed filtering systems on a voluntary basis, the German government chose a more restrictive policy to force Internet Service Providers by law to install filters handed out by the German Federal Criminal Investigation Agency *Bundeskriminalamt* (BKA).

5.3.2 The German Filter Debate

On 17 May 2009, the German Minister of Family Ursula von der Leyen signed an agreement with five of the seven biggest ISPs in Germany to block websites that contained CP material (Krempl 2009c). This agreement was the result of long negotiations between the ruling party CDU and the ISPs and not all of the companies supported the arrangements with the government. The ISPs Freenet and 1&1 declared the lack of a legal basis for such an agreement made it difficult for them to accept the contract. Also civil society organizations like the Chaos Computer Club or MOGIS[53] (representing victims of child abuse) stated their opinions in this debate which were not in favor of the governmental approach. Their central arguments were the lack of consequence by just cloaking websites which would not solve the problem, and the risk of introducing censorship on the Internet. And in deed the plans of the Ministry did not include democratic control of what was going to be filtered (Biermann 2009b).

Unlike most other countries (among the exceptions were Finland and Italy) Germany was going to force the remaining ISPs by law to participate in the filter regime. In the months before, the agreement was based on (more or less) mutual understanding. And with the majority of the big ISPs participating in it, also the big majority of the users had to live with it. On a voluntary basis the companies Deutsche Telekom, Vodafone/Arcor, Alice/HanseNet, Kabel Deutschland and Telefonica O2 Germany who altogether represented 75% of the German market signed the agreement (Schuler 2009).

To create a nationwide filter system Minister von der Leyen initiated a legislative procedure which resulted in the German Internet filter law (*Zugangserschwerungsgesetz*). The objective of the law was to provide German ISPs (strictly speaking Internet access providers) which had at least 10.000 clients with a list containing IP numbers, domain names and URLs that had to be blocked. During the blocking process a block page would appear showing a stop sign which became a symbol for the debate in Germany (Figure 12).

[53] MOGIS is the abbreviation for “Missbrauchsopfer gegen Internetsperren“ (Victims of abuse against Internet blocking).

Figure 12: German Block Page

The German block page was designed to appear in the browser when users were trying to enter a website listed by the BKA because of CP content. The text is informing users about the reason of the website being blocked. Furthermore a contact email is given in case users want to complain about the blocking of a specific site. It is also mentioned that no user data (including the IP address) is saved by the BKA. During the debate on the filter law government representatives requested the identification and prosecution of any user ending up on the block page. This detail was later revised after the proposers were informed that on the Internet any user can be directed automatically to any URL without proper intention.

Source: http://www.cyber-magazin.de

The content of the filter list was to be kept secret. The only instance to administrate the content of the blocklist was the Federal Criminal Investigation Agency BKA. In June 2009 the law was passed in one of the two German chambers (*Bundestag*) by the then ruling coalition of Christian democrats (CDU/CSU) and social democrats (SPD). Except for a small number of members from the Green party the parliamentary opposition opposed the law (Chip Online 2009). In July 2009 also the second chamber (*Bundesrat*) accepted the new law. However, before coming into effect by signature of President Köhler, national elections changed the scenario three months later. The new government was to be formed by Ursula von der Leyen's party CDU together with the liberal FDP which already in the months before, during the discussions on the law had stated its opposition towards Internet filtering. As a precondition to enter the new coalition the party made clear that it was not supporting the Internet filter law. For this reason the CDU decided to put the law on hold (Krempl 2009d). Nevertheless President Köhler was asked for his signature to officially complete the legislative process. He accepted to sign the law in February 2010 after having denied his signature during the first occasion in November 2009. However, the law never came into effect as two months after the President's signature the liberal FDP achieved the abandoning of the law and the ruling coalition decided to replace it with the efforts to delete instead of filtering CP (Berg;

Rosenbach 2010).

5.3.2.1 Supporters and Opponents

The most important argument that Minister von der Leyen and other supporters of the filter law brought into the debate was the fact that as members of government they were obliged the become active against CP on the Internet. Notwithstanding all critics they could not lean back and refuse any activities just because they might turn out to be of little effect. A national government that would not try the least thing possible to solve the problem of CP online would be confronted with much harsher critics than it happened to Minister von der Leyen who became a symbol for online censorship during the debate. In this context the argument of re-victimization is of major importance. It describes the double effect of abuse once during the production of the material and later again during the unlimited access on the Internet. In case the respective material is hosted on a provider outside a country's national borders, filtering could be seen in a first moment as a possible method to inhibit access. On the other hand it also reveals a crucial problem of the public sector not knowing how to find a balance between Internet regulation and civil rights. To a considerable extent this goes back to a lack of knowledge about the latest standards of information technologies.

During the debate members of the BKA justified the law stating that the biggest group of CP consumers was not part of organized child abuse circles whose members would put energy into findig ways to go around the filters. BKA President Jörg Ziercke estimated that 80% of the consumers of CP websites would be scared off by a stop sign on a block page and give up looking for such content (Tagesspiegel 2009). The rest of the users he classified as sophisticated users who would try to go around the filters. Following Ziercke, that group would have to be confronted with further means of investigation. Another BKA argument was the self-regulation of the market. Therefore the reduction of clicks on certain content could be seen on the same level with the reduction of demand and as a next step the ebbing of supply.

On the other hand critics are challenging the supply argument by underlining that a big part of CP material is not traded over websites but within other spheres of the Internet or even on very

traditional ways like the post (Hauck 2009). This is especially the case for producers of such material who work on a commercial level. The communication between producers and buyers happens on the Internet, but the transport of the material on a DVD sent out by snail mail. Only much later after buyers start trading the material with others for free it appears on the Internet. For example on Usenet or on P2P servers which are both not affected by DNS-blocking of CP websites (Bleich; Kossel 2009). And this is the next aspect critics of Internet filter brought up: blocking certain websites that contain CP material will neither significantly influence the commercial market nor really reduce the distribution of the material as the majority is found in other places of the web. In this context also has to be seen the 2008 report of the British Internet Watch Foundation (IWF) which announced an ongoing decrease of CP websites over several years (IWF 2009, p. 7). It stays unclear if the suppliers of such material really left the Internet or if they just switched from websites to other parts of the net. Besides that it is very easy to go around DNS-blockings. Instructions how to do this can be found on several websites on the Internet. They do not have a connection to CP but just deal with the question of filtering in general.

IT security specialists, members of civil society and police investigators in different countries complained about the ineffectiveness of Internet filters, the lack of consistency of public institutions to go against the producers of CP, and the disregard of democratic rights and principles. Hannes Federrath, Professor for Information Security at the University of Regensburg (Germany) criticized filters as "absolutely ineffective" (Biermann 2009a). In his opinion there are more effective methods like working with hash values (algorithms) than using filters (Federrath 2009). Also investigators of the Swedish police showed disappointment regarding the success of the filtering methods implicated in the country. Following the Swedish chief investigator against CP and child abuse, Björn Sellström, the methods introduced to limit access to CP on the Internet did not reach their goal (Donnerhacke 2009). But instead, the number of CP websites on the Swedish filter list has been growing since the system was initiated (Focus Online 2009).

Also representatives of the ISPs admit that filtering does not solve the problem of CP. It just covers the crimes for the public. A more successful way would be clarification and education combined with cooperation with police investigators to persecute the producers and professional distributors. In 2008 German ISPs informed the police in several hundreds of cases about child pornography on the Internet. The question is if these cases are really worked on by the investigators.

Following Christian Bahls from the German organization MOGIS, during the debate on the Internet filtering law German authorities were aware of a variety of servers located in Germany containing CP material. However, they did not become active to close them down (Biermann 2009c). Similar critics regarding the lack of police activities came from the Netherlands where the journalist Karin Spaink found considerable numbers of CP websites that were hosted in the Netherlands, some even appeared on the blocklist of one Dutch ISP but there were no attempts by the police to shut them down. Spaink also pointed out in an article published on her own website, that cooperation between European countries was insufficient. In one case she mentioned the Finnish blocklist included 138 Dutch websites offering CP material. Although both countries are engaged in going against CP their activities were reduced to covering websites than cooperating to investigate against the servers or the producers (Spaink 2008).

The situation of the German government is symptomatic for a large number of governments that are confronted with the challenges of Internet regulation. The decision to filter certain content is easily taken but often lacks the necessary competence towards technological questions. The situation gets worse when political representatives put priorities to gaining votes instead of acquiring the necessary knowledge to resolve contemporary issues. This was also the case with the German filter law which was developed in an unprofessional manner few months before national elections. This problem was confirmed by a leading member of the German government who declared the Internet filter law had become part of the party's election strategy and therefore its implementation was accelerated without taking the technical details into account (Spiegel Online 2009).

As a member of a democratic government Minister von der Leyen should have known that the concerns of introducing an undemocratic procedure would call the attention of civil society actors advocating for privacy issues and freedom of speech. In the Internet era these two topics entered into a new dimension for which none of the political parties (being in power or in opposition) was prepared. This vacuum of competence inside the public sector for developing effective policies on Internet regulation was filled by a number of civil society actors which had a different profile than those actors dealing with similar questions in the past. Since the 1970s privacy advocates had gained substantial importance in Germany. One key event at that time was the controversial debate on the national census that took place in 1987 after massive protests of the

population had lead to a decision of the Federal Constitutional Court confirming the importance of privacy and data protection as a civil right (Schmitt; Wefing 2010). Since that time data protection agencies played an important role as advocates of citizens' personal rights. However, established privacy actors were not prepared for the upcoming challenges caused by a rapid development of cyberspace. For this reason the debate on Internet filters brought a new generation of privacy actors on the political stage which originated in the hacker and IT community. The mobilization of these actors happened for a good part over the Internet itself. An online petition demanding the rejection of the process to pass the Internet filter law reached the necessary quantity of 50.000 votes within four days and was passed on to the German government for reconsideration (Deutscher Bundestag 2009). Overall the petition gained 134.015 signatures making it the most signed petition in the history of the country.

The final decision of the German government to abandon the filter law and to concentrate on deleting CP on the service providers was a major achievement for the opponents of the law. Since the beginning of the debate the main political drivers that were opposing the law had favored this solution. Supporters of Internet filtering doubted the success of deleting the material arguing that due to the transborder character of the Internet it would be difficult or even impossible to delete content on a provider established outside the country. One year after the end of the filter law the German e-commerce association (eco) presented their statistics showing that in 2010 all CP content on German providers was deleted within one day. Regarding international providers this process took some more days due to administrative processes. In this context a focus was given on Russian and U.S. American providers which are hosting the most CP content. Following eco, both Russian and American providers needed little more than one week to delete the material (eco 2010). Also BKA statistics revealed that more than 75% of the content they were aware of could be deleted (Hebestreit 2011).

5.3.3 File Sharing

The growing success of new actors on the political stage was manifested by the expansion of a new political party originally founded in Sweden in the year 2006 named the Pirate Party (PP). Although the PP had a very specialized agenda focusing exclusively on information society and privacy topics it won 7,13% of the Swedish votes in the 2009 elections of the European Parliament. Between 2006 and 2010 similar parties were founded in a number of European countries, among them Denmark, Finland, Germany, Netherlands and Spain, building an international association. The success of the Swedish PP goes back to the conflict on P2P technology which culminated in the process against the torrent service provider The Pirate Bay. The torrent or bittorrent technology became the largest file sharing technology of the early 21st century enabling the fast transfer of large data files (Miegel; Olsson 2008). At the same time it became a serious problem for parts of the entertainment industry as a large number of users exchanged music and movie files via bittorrent technology. As in Sweden privacy legislation made it impossible to trace back Internet users by their IP address the bittorrent technology was widely used and socially accepted, comparable to the home recording of music tapes in the 1980s and 1990s. For this reason the process against The Pirate Bay, initiated by a Swedish court in January in 2008 and supported by the International Federation of the Phonographic Industry (IFPI) caused a wave of support by Swedish Internet users which lead to a massive increase of admissions to the PP. The PP was connected to The Pirate Bay and favored the reformation of intellectual property rights laws to adapt to the reality of the Internet age. At the time the IFPI amplified their legal actions against bittorrent providers, the bittorrent protocol itself was the dominant protocol on the Internet even outrivaling HTTP (Schulze; Mochalski 2009, p. 3).

Parallel to the process in Sweden the IFPI and other defenders of traditional intellectual property rights tried to force ISPs in several countries to block access to The Pirate Bay. However, all efforts to block the website failed as it frequently reappeared on servers in other countries. Even when in April 2009 the Swedish court found the operators of The Pirate Bay guilty of copyright infringement the website remained online.

Influenced by the internationally observed case in Sweden, Internet activists founded branches of the PP in several countries. In Germany the debates on the Internet filter backed the

success of the German PP which was founded in 2006. Even though the party was trivialized for its monothematic program it managed to increase the number of supporters and succeeded to enter the senate in Berlin at the local elections in September 2011. With 8,9% it became the fifth largest party to gain seats in Berlin while at the same time the FDP, one of the ruling parties on the national level, received 1,8% (before: 7,6%) and failed to enter the city parliament in the German capital (Spiegel Online 2011). National polls showed that four weeks after the elections the PP had 7,6% of the votes which would open the doors for the German parliament (Wahlumfrage 2011).

There is no doubt that in the coming years file sharing and infringement of intellectual property rights on the Internet will remain among the central topics within the debate on Internet filtering. The internationally observed discussions on the U.S. draft laws SOPA and PIPA as well as similar debates in other countries are proving that Internet filtering will remain on the political agenda of Internet governance actors. As the time frame of this thesis ends in 2010 this topic will not be deepened in here. However, it shows that the aspects discussed within the time frame are representing the beginning of an intense debate which can be investigated in future research projects.

Chapter Six: Conclusion

When the Working Group on Internet Governance published the first widely accepted definition of Internet governance in 2005 it included several stakeholder groups from the public sector, the private sector and civil society which underlined the fact that at that time it was already clear that numerous interest groups were involved in the development and regulation processes of the global network. These constellations became obvious after the commercialization of the Internet had begun in the early 1990s when in fact the Internet governance process was starting to evolve. Although at that time the expression “Internet governance” was still unknown. Before the commercialization had started (and especially in the early days of computer networking) there were mainly a few public institutions and researchers in the U.S. involved in the whole project, plus a small number of individuals or organizations in other countries. The expansion of the Internet in every area of connected societies created a plurality of interest groups whose numbers were increasing parallel to growing technical innovations. Over the years, the early actors like ARPA, the NSF and a number of universities were joined by organizations from the private sector looking to expand their traditional business models on the Internet or those companies that were founded as online enterprises. Also governments from all over the world recognized the importance to join debates concerning the Internet. And the more they became involved in it the more they tried to control it, independently if they were considered democratic or not. And also civil society actors joined the scene to improve their own activities by using the Internet, by including it into their agenda of activities and also (just as newly founded online enterprises) new NGOs and similar organizations appeared which had the Internet itself as the main focus of their efforts.

One of the first big challenges and also one of the biggest conflicts of Internet governance in the 1990s was the establishment of ICANN as a technical regulation body. Since the foundation of the Internet was laid in the United States and its early innovations happened mainly in the U.S. as well, it became obvious that the country would also want to play a major role in the technical regulation processes. Especially as Washington had realized quickly how its own economy could benefit from the new technology. Though, due to the conflicts that had arisen in the years before (e.g. during the MoU process), the U.S. government had realized that a large number of participants and an open process of discussion regarding the new organization that was going to be established was necessary to create a stable environment for the Internet to grow. For this reason the debates

about the Green and the White Paper happened in an open environment where any individual interested could state its concerns, critics and ideas which were then considered (at least partly) for further proceedings. This approach was highly necessary as it was impossible for a few single actors or even within a traditional public sector policy making process to consider all the details regarding the technical environment, intellectual property rights, security issues, human rights and more. Especially as in the following years the public sector frequently proved itself uncapable when it came to resolve urgent questions of the Internet like weighing up intellectual property rights protection and freedom of speech as it became clear for example during the European discussions about Internet filtering.

The fact that ICANN was established in the United States based on U.S. legislation and under control of the U.S. government (via DOC) remained an important reason for its critics to watch carefully how and which decisions were taken by the organization over the years. At the same time ICANN tried to include as many stakeholder groups as possible into its organizational body and started experimenting with new forms of participatory procedures like online elections in the year 2000. However, political analysts like Milton Mueller constantly underlined the problem that ICANN's policies (for example regarding the JPA) were going in line with Washington's political interests. The fact, that Washington constantly renewed the JPA over the period of ten years instead of reducing its control over crucial Internet regulation bodies did not contribute to a possible increase of trust between Washington and a large part of the international Internet community. Tensions might decrease in the following years since the JPA was replaced by the more liberal AoC. Nevertheless, the conflict about U.S. control over IANA is continuing. Reflecting on the efforts of the U.S. government it is interesting to mention that over the years Washington's attitude towards Internet control has changed insofar that in the early days it tried to maintain control over the Internet to make sure it could develop in an unregulated environment while in the early 21st century control over the Internet by Washington (and other governments) was more focused on the question of how to regulate it. This recent development gets reflected especially in the debates on Internet filtering and the protection of intellectual property rights. But also debates on cybercrime are dealing with the question of control. In some cases cybercrime and Internet filtering are even related to another as policy makers try to establish filter regimes to combat certain forms of online crime.

The spreading of cybercrime naturally happened parallel to the spreading of the Internet. Since the 1990s there has been an increase in quantity and quality of cybercrime on the Internet. While the early cyber delinquents concentrated on personal gains, an industry of cybercriminals has developed over the years. The professionalization of this environment has lead to a situation in which delinquents hire services of other delinquents to pursue their own financial interests. This means that cybercriminals specialized in phishing or credit card fraud concentrate on obtaining passwords or credit card numbers which are then offered to anyone interested in using them for further criminal activities. The same way bot herders offer their botnets to those who are willing to pay for them. The problem of botnets is increasing as they are not only interesting for ordinary cybercriminals who are trying to make financial profits from them but also to groups or individuals with a political agenda. The botnet phenomenon demonstrates the connection between ordinary criminal actors and those that are using cyber attacks (especially DDoS attacks) for ideological reasons. This means the problem of politically motivated cyber attacks is directly linked to ordinary cybercrime.

The cyber attacks on Estonia and Georgia are underlining this relation. In both cases DDoS attacks were conducted on a large scale which required access to professional botnets as they are offered by cybercriminals. Although technically it would be possible to set up botnets on a legal basis it is very unlikely that any actor willing to conduct cyber attacks would connect thousands of computers in his own possession to form a botnet. The financial and logistical requirements would be too high to realize such a plan (although it is not impossible that in the future governments would become interested in doing so). For this reason any politically motivated cyber attack has a direct relation to cybercriminal actors. It is not possible to separate politically motivated DDoS attacks from cybercrime.

Even in case individual governments would become interested in the future in forming their own botnets on a legal basis there is no doubt so far, that officially cybercrime is a problem for any government and economy as it is causing serious damage to a large number of enterprises and public institutions as well. However, unofficially governmental actors might very well be involved in cyber criminal activities like breaking into foreign networks with the intention of espionage or even sabotage as the case of Stuxnet has shown. So far, there is no adequate legislation concerning cyber threats in most countries. Therefore, it remains undefined if a hacking tool or malware code

developed by cybercriminals turns to be a “legitimate” means to defend national interests once it gets into possession of a secret service. The debate on this question is doubtlessly going to appear on the agenda of several states in the next years, also in relation with the debate on cyberwar. In this context it needs to be discussed what defines a cyber attack on a state and which would be an adequate response. Most probably certain cybercrime tools will then be defined as legitimate weapons of self-defense. In fact, the first steps for this debate have already been taken in the U.S.

Much more than traditional crime, cybercrime requires international cooperation. The fact that criminal activities can be conducted independently of time and location underlines the necessity of international agreements to harmonize national legislations and to facilitate the transnational prosecution of cybercriminals. For this reason a large number of International and Regional Organizations has put the problem of cybercrime on their agenda. The result is a huge amount of recommendations, declarations and action plans of which few have reached a wider international recognition. Among those are the 24/7 Network of High Tech Points of Contact and the Budapest Convention on Cybercrime. While the 24/7 Network is an informal association of contact points in a number of countries that build an international network of cybercrime experts which are available also in cases of emergency, the Budapest Convention is so far the leading international document which governments refer to when preparing their national legislation for the combat against the latest Internet crimes. Until October 2010 the Budapest Convention was signed by 46 governments. However, strategically important countries like Russia (which is home to a highly active cybercriminal scene) did not join the list of supporters. Instead, critics (among them Russia) suggested to develop an alternative document which was refused especially by European and North-American supporters of the Budapest Convention. Until 2010 no readiness to negotiate about this blockade among the traditional adversaries could be observed.

Similar to the scenario of traditional crime, also in cybercrime there is less space for civil society than for security forces and the law. So far, this space is even smaller for civil society when comparing ordinary crime to cybercrime. In the first twenty years of the commercial Internet there was, for example, no significant engagement of NGOs to prevent people from getting involved in cybercrime. While street crime prevention is often realized by showing concern for potential delinquents this is not the case for cybercrime. Little is known on the academic level about the profiles of cyber criminals. However experience show that they are of relatively young age, mostly

male and necessarily possess advanced knowledge of information technologies. Instead of becoming engaged in cybercrime prevention among peer groups of potential offenders, civil society actors focus more on the victims of cybercrime. In this context, they concentrate on information campaigns among possible victims which are of course much easier to identify than possible offenders. One field in which civil society actors show high engagement is the area of child pornography which appears in the debates on cybercrime as well as in the debates on Internet filtering. It is even possible to say that child pornography is connecting these two sub-fields of Internet governance by being a cybercrime that caused the increase of the discussions on Internet filters.

Another observation regarding civil society is the question if (more or less) organized hacker groups can be considered civil society actors or not. The rise of the Internet witnessed the formation of innumerous hacker groups of which some are obviously part of the cyber delinquent scene while others could be considered social groups defending the interests of Internet users. These groups and collectives are located in a legal limbo and are neither cybercriminals nor traditional civil society actors.

When it comes to the Internet filter scenario the functions of the different stakeholder groups are better defined than in the cybercrime scenario with its high quantity of invisible actors. One important reason is that stakeholders in Internet filtering themselves are to some extent clearly arranged. In this context parts of the software producing industry have a key function. The quantity of producing companies is relatively small and most of them are located in the U.S. The products they are developing do not necessarily aim at supporting censorship in a classical sense which means limiting freedom of the press and freedom of speech regarding basic political rights. Moreover their original objective was to block content that was considered inappropriate for example for minors, being especially adult content. However, the application of such software products in public institutions like schools and libraries also caused discontent by those defending the access to all kinds of information as a basic right in the U.S. (where the first filters were installed in the 1990s). In addition, the problem of overinclusiveness and underinclusiveness turned simple filter techniques into tools of unwanted censorship in which websites were blocked just because of certain keywords, independent of their actual content. Over the years these products became increasingly known also in countries whose governments tend to censor political and social

information in their national medias. This way, Western software products became part of censorship regimes in a variety of countries all over the world. Although none of the producing companies favored this way of applying their products they saw themselves confronted with heavy criticism about supporting censorship. The dual-use function of certain products put companies like CISCO and others in the position of suspects delivering censorship technology to authoritarian regimes. These companies became caught between the commitment to democracy and the desire to participate in new and growing markets in the world which were often situated in non-democratic countries. Although the software industry can be considered a strategic actor in the Internet filtering scenario there are also other interests from actors of the private sector like the entertainment industry which is favoring Internet filtering and other forms of Internet control to guarantee their continuing economic growth.

Regarding the public sector there are many non-democratic countries which became symbols for Internet filtering in the early 21st century. Especially China was widely mentioned for its rigid filter regime. But as research results of the OpenNet Initiative showed, a large number of countries besides China started using Western technologies to censor the Internet. In Western democratic countries reactions to these developments were harsh. Governments in several Central- and East-Asian countries but also in the Middle East and North-Africa were criticized for their restrictions on the Internet. Nevertheless it needs to be mentioned that Internet filtering or Internet censorship in those countries are merely the adaption of already existing limitations of freedom of speech which before the spreading of the digital age were basically concentrated on printed publications or public events. The transfer of the already existing restrictions to the online environment is therefore simply a consequent continuation of formerly implemented restrictive policies. What is interesting to mention is the growing variety and professionalization of Internet filtering practices. While only a few years ago authoritarian governments mostly applied simple methods like keyword filtering to control the flow of information inside their countries' networks, this has changed quickly. Already in 2010 more effective forms of filtering were applied, together with new forms of Internet surveillance which will become crucial methods of information control in the coming years. Two important aspects for further research in this area are the investigation of deep-packet inspection (not only in context of non-democratic countries) and the very recent phenomenon of IDN ccTLDs and its possibilities to improve information control systems.

A somehow different (but to critics also similar) situation an be detected when taking a look at democratic governments, mainly in Western Europe and North America. While in those countries the discourse on Internet filtering was in the 1990s and in the beginning of the new millennium focused on a critical observation of Internet filter regimes in non-democratic countries (with few exceptions regarding the U.S. library cases), there was a shift between 2004 and 2010. In that period democratic governments started to develop filtering regimes for their own networks, mainly justified by online content of child abuse. The debate on Internet filtering in democratic countries resulted in a growing opposition against the governmental plans, fueled by the technical incompetence of government representatives and the fear of an evolving censorship regime based on populist justifications and besides that pushed by a number of entertainment companies which for a long time had been lobbying governments to develop restrictive Internet policies regarding file sharing and other activities that caused loss to their traditional business models. The controversial debate resulted in an appearance of former civil society actors in the public sector which especially in Europe caused a certain shift in the scenario of traditional political parties. The fact, that a mono-thematic party (like the Pirate Party) managed to multiply the number of members and supporters in several countries within months and even successfully participated in election processes demonstrates the growing interest of voters for the challenges of the digital age. It is unclear so far, how this scenario will develop in the future. One important question is if digital topics will remain of high interest for the voting population which is very likely to happen as the Internet and other forms of ICT can be considered permanent technologies constantly spreading in any corner of modern societies. Another question is how traditional political parties will manage to improve their lack of competence in the digital field. Looking at the example of Germany one can see that the first reactions of mockery by traditional parties towards the unconventional appearance of the new Internet-focused party (comparable to the attitude towards the Green Party in the 1980s) were quickly replaced by attempts of traditional parties to improve their approaches towards modern ICTs.

The role of civil society in the context of Internet filtering is focusing on what can be considered classical functions of civil society organizations, being mainly the representation and advocacy of citizens' rights and the contribution of expertise. In the wider context of Internet filtering (and other forms of surveillance) there are those organizations (mostly NGOs but also other forms like expert groups) that included Internet topics into their already existing agenda like

classical human rights NGOs and those that were formed with a special focus on Internet policies. In cases of filtering regimes in non-democratic countries there is a wide consensus among civil society organizations criticizing censorship and the prosecution of Internet users, bloggers or journalists while the focus of the debate is mainly set on human and basic rights violations (especially freedom of speech and freedom of the press). At the same time debates on Internet filtering in democratic countries have a quite different character. Not classical human rights NGOs but technical expert groups and users are dominating the debate in the civil society sector. Different to authoritarian regimes, democratic governments are not threatening the physical integrity of Internet users but mainly the freedom of the network itself (net neutrality) and by doing so they are limiting the rights of the Internet user. Activists are fearing the introduction of a censorship regime that starts with a widely accepted target (child pornography) but later could be expanded to political or religious content. And in fact, there is a high probability that restrictive Internet filtering policies will be extended to other topics than child abuse, once the infrastructure is established. Besides that the problem of overinclusiveness is a serious issue that will automatically lead to censorship of individual websites as the library cases in the U.S. have shown. The fact, that over the years civil society organizations (especially those with a strong Internet policy approach) have proven their competence regarding technical issues of the Internet, has made them interesting and reliable partners for both the public and the private sector in democratic countries in case they were in need of professional assistance or even for reasons of public relations. On the other hand civil society actors could become serious opponents especially for the public sector in case of restrictive Internet filtering policies.

The Internet governance process between the years 1990 and 2010 has been driven by a plurality of actors from all sectors of society. When comparing different decision or policy making processes during these years it becomes clear that the inclusion of a wide variety of actors has also lead to a more stable environment for processes of regulation. This could be seen for example during the constitution process of ICANN, the Green Paper and the White Paper process, in which concerns and findings from all interest groups were brought in and discussed to develop a solution based on the most comprehensive compromise possible. In contrast, the previous efforts to privatize the DNS happened (basically for political reasons) in more exclusive environments and failed, also due to lack of support by the excluded actors. To avoid these conflicts the multi-stakeholder governance model has become a universally accepted governance model within the Internet

governance community. A major reason for this is its application in the Internet Governance Forum which during its first mandate from 2006 to 2010 managed to spread the idea of multi-stakeholderism to Internet governance actors in all parts of the world which then applied it in their own regional contexts. Also the debates and conflicts in the areas of cybercrime and Internet filtering, as analyzed in this thesis, benefited from this approach. For example, the debates on filtering, especially in Europe and North America have shown that solo attempts by the public sector to develop Internet policies cause not only discontent but can also result in technical failures and damages to the functioning of the Internet itself. However, although the multi-stakeholder approach has been established as a widely accepted governance model, it has been challenged by a number of governments which prefer to develop their national Internet policies without consulting other parts of society. The following years, and also the developments during the second IGF mandate, will show, if the multi-stakeholder governance model will prevail and if the Internet governance process might become a role model for governance processes in other policy fields.

Capítulo Seis: Conclusão

Quando WGIG publicou a primeira definição de governança da internet que foi amplamente aceita em 2005, foram incluidos diversos atores do setor público, do setor privado e da sociedade civil, o que destacava o fato de que já naquele momento estava claro que um número grande de atores foi envolvido no desenvolvimento e nos processos de regulamentação da rede global. Estas constelações ficaram óbvias após o começo da comercialização da internet no início de 1990, quando de fato o processo de governança da internet começou a se desenvolver. Apesar disso, naquele momento a expressão "governança da internet" ainda não era empregada. Antes do início da comercialização (e em especial nos primórdios da rede de computação) haviam poucas instituições publicas e pesquisadores nos EUA envolvidos em todo o projeto, adicionando-se a isto um pequeno número de indivíduos e de organizações de outros países. A expansão da internet em todas as áreas da sociedade conectada criou uma pluralidade de atores cujos números cresciam paralelamente as crescentes inovações técnicas. Ao longo dos anos, os atores iniciais como ARPA, a NSF e um número de universidades foram unidos por organizações do setor privado buscando expandir seus modelos de negócios tradicionais na internet ou organizações que foram fundadas como negócios online. Governos do mundo inteiro reconheceram a importância de fazer parte de debates que envolviam a internet. Quanto mais eles se envolviam, mais eles tentavam obter controle, independentemente de serem considerados democráticos ou não. Atores da sociedade civil também se uniram ao cenário para a melhoria de suas próprias atividades por intermédio da internet, ao acrescentar suas agendas de atividades e também (assim como as empresas recentemente fundadas na internet) novas ONGs e organizações semelhantes surgiam com a internet como seu foco principal em concentração de esforços.

Um dos primeiros grandes desafios e também um dos maiores conflitos da governança da internet foi o estabelecimento da ICANN como um corpo técnico regulador em 1990. Desde que a internet foi fundada nos EUA e suas inovações iniciais aconteceram lá também, tornou-se claro que o país gostaria de desempenhar um papel de destaque nos processos de regulamentação técnica. Especialmente quando Washington percebeu rapidamente como a nova tecnologia poderia beneficiar sua economia. Embora, devido aos conflitos que surgiram nos anos anteriores (por exemplo: durante o processo de MoU), o governo dos EUA havia percebido que um grande número de participantes e um processo de discussão aberta envolvendo o estabelecimento da nova

organização eram necessários para criar um ambiente estável para o crescimento da internet. Por esse motivo os debates sobre os Livros Verde e Branco aconteceram em um ambiente aberto, onde cada indivíduo podia declarar suas preocupações, suas críticas e idéias que eram levadas em conta (pelo menos parcialmente) para futuros procedimentos. Essa abordagem era altamente necessária, já que era impossível fazer com que poucos atores ou até mesmo grupos tradicionais do setor público de decisões políticas levassem em consideração todos os detalhes do ambiente técnico, direitos de propriedade intelectual, questões de segurança, direitos humanos, e mais. Especialmente porque, nos anos seguintes o setor público frequentemente se mostrou incapacitado diante da necessidade de solução de questões urgentes da internet como fazer uma pesagem da proteção dos direitos de propriedade intelectual e da liberdade de expressão, como se tornou claro durante as discussões da Europa sobre filtragem na internet.

O fato da ICANN ter sido estabelecida nos EUA, baseada na legislação Americana e sob controle do governos estadunidense (via DOC) se manteve como uma forte razão para uma observação cuidadosa por parte de seus críticos de como e quais decisões eram tomadas pela organização ao longo dos anos. Ao mesmo tempo a ICANN tentava incluir o máximo de atores possível no corpo da organização e iniciou experiências com novas formas de procedimentos de participação como eleições online em 2000. No entanto, analistas políticos como Milton Mueller ressaltavam o problema das políticas da ICANN (por exemplo em relação ao JPA) frequentemente se alinharem aos interesses políticos de Washington. O fato, que Washington constantemente renovava o JPA em períodos de dez anos em vez de reduzir seu controle sobre corpos de regulamentos cruciais da internet não contribuiu para um possível aumento de confiança entre Washington e grande parte da comunidade internacional da internet. As tensões poderiam diminuir nos anos seguintes desde que o JPA foi substituído pelo AoC que era mais liberal. No entanto, o conflito em relação ao controle dos EUA sobre IANA continua. Refletindo sobre os esforços do governos dos EUA é interessante mencionar que ao longo dos anos a atitude de Washington em relação ao controle da internet tem mudado na medida em que nos primeiros dias ele tentou manter um controle sobre a internet para garantir que pudesse se desenvolver em um ambiente desregulamentado enquanto que no começo do século 21 o controle de Washington (e outros governos) era mais focado na questão de como regulamenta-la. Esse desenvolvimento recente é refletido principalmente nos debates de filtragem na internet e de direito de proteção de propriedade intelectual. Mas debates do crime cibernético também lidam com a questão do controle. Em alguns

casos o crime cibernético e a filtragem na internet são até mesmo relacionados um ao outro quando formadores de política tentam estabelecer um regime de filtragem de combate aos crimes online.

A difusão do crime cibernético aconteceu paralelamente à expansão da internet. Desde 1990 houve um aumento na quantidade e na qualidade do crime cibernético na internet. Enquanto os primeiros delinqüentes cibernéticos concentravam-se em ganhos pessoais, uma indústria de criminosos cibernéticos se desenvolveu ao longo dos anos. A profissionalização desse ambiente levou a uma situação em que delinqüentes contratam serviços de outros delinqüentes para atingir seus próprios interesses financeiros. Isso significa que criminosos cibernéticos especializados em phishing ou em fraudes de cartões de crédito se concentram na obtenção de senhas ou números de cartão de crédito que são então oferecidos a qualquer um interessado em seu uso ou para mais atividades criminosas. Da mesma forma bot herders estão ofereçendo seus botnets aos que estão dispostos a pagar por eles. O problema dos botnets está crescendo já que eles não são só interessantes para criminosos cibernéticos comuns que buscam benefícios financeiros mas também para grupos e indivíduos com uma agenda política. O fenômeno dos botnets demonstra a conexão entre atores criminosos comuns e aqueles que usam os ataques cibernéticos (especialmente ataques DDoS) por razões ideológicas. Isso significa que o problema de ataques cibernéticos com motivações políticas está diretamente ligado ao crime cibernético comum.

Os ataques cibernéticos na Estônia e na Geórgia ressaltam essa relação. Em ambos os casos os ataques DDoS foram conduzidos em uma ampla escala, que requeria acesso a botnets dos profissionais de crime cibernético que o oferecem. Apesar da possibilidade de preparo de botnets de forma legal é muito improvável que qualquer ator disposto a preparar ataques cibernéticos conectasse milhares de computadores de posse própria para formar um botnet. Os requerimentos financeiros e logísticos seriam muito altos para a realização desse plano (apesar da possibilidade de interesse futuro por parte dos governos). Por esse motivo qualquer ataque cibernético com motivação política tem relação direta com criminosos cibernéticos. Não é possível separar ataques cibernéticos DDoS com motivações políticas do cibercrime.

Mesmo no caso de governos se interessarem na formação de suas próprias botnets de forma legal no futuro, não há dúvidas até então que o cibercrime se tornou oficialmente um problema para qualquer governo e para qualquer economia já que tem causado sérios danos a um grande numero

de empresas e instituições públicas. No entanto, atores não oficiais do governo podem estar envolvidos em atividades de crime cibernético como a invasão de redes estrangeiras com a intenção de espionagem ou até mesmo de sabotagem, como mostrado no caso da Stuxnet. Até agora, não há legislação adequada em relação a ameaças cibernéticas na maioria dos países. Portanto, permanece indefinido se uma ferramenta de hacking ou um código de malware desenvolvido por criminosos virtuais vem a ser um meio "legitimo" de defesa dos interesses nacionais uma vez que chega a posse de um serviço secreto. O debate dessa questão sem dúvida vai parecer na agenda de diversos estados nos próximos anos, também em relação ao debate de guerra cibernética. Nesse contexto é necessário que se discuta o que define um ataque cibernético a um estado e o que seria uma resposta adequada. Muito provavelmente, algumas ferramentas do cibercrime serão então definidas como armas legítimas de autodefesa. De fato, os primeiros passos para esse debate já foram tomados nos EUA.

O crime virtual requer muito mais cooperação internacional do que o crime tradicional. O fato de que as atividades criminosas podem ser conduzidas independente do tempo e espaço ressalta a necessidade de acordos internacionais para a harmonização de legislações nacionais e para facilitar a acusação de criminosos virtuais. Por esses motives existem grandes números de organizações internacionais e regionais que colocaram o problema do crime cibernético em suas agendas. O resultado é um grande número de recomendações, declarações e planos de ação dos quais poucos alcançaram um reconhecimento internacional mais amplo. Entre estes estão a Rede de Pontos de Contato de Alta Tecnologia 24/7 e a Convenção de Crime Cibernético de Budapeste. Enquanto a Rede 24/7 é uma associação informal de pontos de contato em numerosos países que constroem uma rede internacional de experts no cibercrime que estão disponíveis também em casos de emergência, a convenção de Budapeste está formando um documento internacional ao qual governos se referem ao formularem sua legislação nacional para o combate dos últimos crimes da internet. Até Outubro de 2010 a Convenção de Budapeste foi assinada por 46 governos. No entanto, países estrategicamente importantes, como a Rússia (que é sede de um cenário do cibercrime altamente ativo) não se uniram a lista de apoiadores. Ao invés disto, críticos (entre eles a Rússia) sugeriram o desenvolvimento de um documento alternativo que foi recusado, em especial por apoiadores Norte Americanos e Europeus da Convenção de Budapeste. Até 2012 não foi observada nenhuma disposição para negociar sobre esse bloqueio entre os adversários tradicionais.

Semelhante ao cenário de criminologia tradicional, também no cibercrime há menos espaço para a sociedade civil do que há para as forces de segurança e a lei. Até agora, esse espaço é ainda menor para a sociedade civil quando se compara o crime comum ao crime cibernético. Nos primeiros vinte anos de comercialização da internet não houve, por exemplo, um comprometimento significativo de ONGs para prevenir que pessoas se envolvessem no cibercrime. Enquanto a prevenção de crimes de rua é geralmente feita através da demonstração de preocupação com delinqüentes em potencial esse não é o caso do crime cibernético. Sabemos pouco no nível acadêmico de perfis de criminosos virtuais. No entanto, a experiência nos mostra que eles tem relativamente pouca idade, em maior parte homens e sempre possuem um conhecimento avançado de tecnologia da informação. Ao invés de se comprometer com a prevenção de crimes cibernéticos entre grupos de ofensores potenciais, os atores da sociedade civil focam mais nas vitimas do crime cibernético. Nesse contexto, eles se concentram em campanhas informativas a possíveis vítimas que são obviamente muito mais fáceis de identificar do que ofensores potenciais. Um campo no qual atores da sociedade civil demonstram um alto comprometimento é a área de pornografia infantil que aparece em debates sobre o crime cibernético e em debates da filtragem na internet. É até mesmo possível dizer que a pornografia infantil está unindo campos de governança da internet sendo um crime cibernético que causou um aumento de discussões sobre filtragem na internet.

Outra observação sobre a sociedade civil é a questão de se grupos de hackers organizados podem ser considerados atores da sociedade civil ou não. A ascensão da internet testemunhou a formação de inúmeros grupos de hackers dos quais alguns são obviamente parte do cenário de delinqüentes cibernéticos enquanto outros podem ser considerados grupos sociais defendendo parte de seus interesses e dos interesses de outros usuários da internet. Esse grupos estão localizados em um limbo legal e não são nem criminosos virtuais nem atores tradicionais da sociedade civil.

Quando se trata do cenário de filtragem na internet, as funções dos atores diferentes são mais bem definidas do que no cenário do crime cibernético com sua grande quantidade de atores invisíveis. Uma razão importante é que os interessados na filtragem na internet em si são até certo ponto muito bem organizados. Nesse contexto as partes da indústria de produção de software tem uma função chave. A quantidade de empresas produtoras e relativamente pequena e a maioria está localizada nos EUA. Os produtos sendo desenvolvidos não focam necessariamente em dar apoio a censura em um sentido clássico, o que significa limitar a liberdade de imprensa e liberdade de

expressão em relação aos direitos políticos básicos. Seu objetivo inicial era o bloqueio de conteúdo que fosse considerado inapropriado por exemplo para menores, geralmente conteúdo específico para adultos. No entanto, a aplicação de softwares desse gênero em instituições como escolas ou bibliotecas também causou um descontentamento entre aqueles que defendiam acesso a todas as formas de informação como um direito básico dos EUA (onde os primeiros filtros foram instalados em torno de 1990). Além disso o problema de *overinclusiveness* e de *underinclusiveness* tornou técnicas de filtragem simples em ferramentas de censura desprezadas na qual sites eram bloqueados apenas por causa da inclusão de certas palavras chaves, independente de seu conteúdo real. Ao longo dos anos o conhecimento desses produtos aumentou também em países nos quais o governo tende a censurar informações políticas e sociais a suas mídias nacionais. Dessa maneira, os produtos de software ocidentais se tornaram parte de regimes de censura ao redor do mundo. Embora nenhuma das empresas produtoras tenha favorecido essa maneira de aplicar seus produtos, elas se viram confrontadas com uma crítica forte sobre o apoio a censura. A função dupla de utilização de certos produtos colocou empresas como a CISCO e outras em uma posição de suspeita de entrega de tecnologias para a censura em regimes autoritários. Essas empresas se viram encurraladas entre o comprometimento com a democracia e o desejo de fazer parte de mercados novos e crescentes no mundo, que muitas vezes estavam situados em países não democráticos. Apesar da indústria de software ser considerada um ator estratégico no cenário de filtragem na internet, também há outros interesses de atores do setor privado como a indústria do entretenimento que favorece a filtragem na internet e outras formas de controle para garantir seu crescimento econômico.

Em relação ao setor público existem muitos países não democráticos que se tornaram símbolos da filtragem na internet no inicio do século 21. A China em especial foi amplamente mencionada por seu regime de filtragem rígido. Mas como mostram os resultados de pesquisa da OpenNet Initiative, um grande número de países além da China começou a utilizar-se de tecnologias ocidentais para a censura da internet. Em países democráticos ocidentais as reações a esses avanços foram severas. Os governos de países da Ásia Central e do leste da Ásia, assim como leste e norte da África foram criticados por suas restrições na internet. No entanto, deve ser mencionado que a filtragem na internet ou a sua censura nesses paises são apenas uma adaptação das limitações já existentes de liberdade de expressão, que antes do avanço da era digital estavam concentradas em publicações e eventos públicos. A transferência das restrições já existentes para o ambiente online é portanto simplesmente uma conseqüência que extende das políticas restritivas

implementadas anteriormente. É interessante mencionar a variedade crescente e profissionalização de filtragem na internet. Enquanto a poucos anos atrás governos autoritários aplicavam métodos simples como a filtragem de palavras chave para o controle do fluxo de informação em seus países, isso mudou rapidamente. Já em 2010 formas mais efetivas de filtragem foram aplicadas, junto a novas formas de vigilância da internet, o que se tornará métodos cruciais de controle da informação nos próximos anos. Dois aspectos importantes para futuras pesquisas nessa área são a investigação de *deep packet inspection* (não só no contexto de países não democráticos) e o fenômeno recente da IDN ccTLDs e suas possibilidades de aprimoramento dos sistemas de controle de informação.

Uma situação um tanto diferente (mas para os críticos também semelhante) pode ser detectada com a observação de governos democráticos, em sua maior parte na Europa Ocidental e na América do Norte. Enquanto nesse países o discurso sobre a filtragem na internet foi nos anos 90 e no inicio do novo milênio focando em uma observação critica de regimes de filtragem na internet em países não democráticos (com poucas exceções relacionadas por exemplo aos casos de bibliotecas dos EUA), houve uma virada entre 2004 e 2010. Naquele período governos democráticos começaram a desenvolver regimes de filtragem para suas próprias redes, justificado principalmente pelo conteúdo de abuso de crianças online. O debate de filtragem na internet em países democráticos resultou em uma oposição crescente aos planos governamentais, impulsionada pela incompetência técnica de representantes governamentais e pelo medo de um regime de censura crescente baseado em justificativas populistas e além disso impulsionados por empresas de entretenimento que há muito tempo davam entrada em pedidos aos governos de desenvolvimento de políticas restritivas da internet em relação ao compartilhamento de arquivos e outras atividades que traziam perdas aos seus modelos de negócio tradicionais. O debate controverso resultou na aparição de ex-atores da sociedade civil no setor público, os quais causaram uma certa mudança no cenário tradicional de partidos políticos especialmente na Europa. O fato, de um partido mono-temático (como o Partido Pirata) ter multiplicado o número de membros e apoiadores em vários países em meses e até ter participado com sucesso de processos de eleição, demonstrou o interesse crescente de eleitores pelos desafios da era digital. É incerto até agora como esse cenário vai se desenvolver no futuro. Uma questão importante é se tópicos do espectro digital permaneceram no interesse da população eleitora, o que muito provavelmente acontecerá como a internet e outras formas de TICs podem ser consideradas tecnologias permanentes em constante crescimento em qualquer canto das sociedades modernas. Outra questão é como os partidos políticos tradicionais irão gerenciar o

aprimoramento em sua falta de competência no campo digital. Ao observar o exemplo da Alemanha pode-se ver que as primeiras reações de zombaria pelos partidos políticos tradicionais diante do partido novo focado na internet (comparável a atitude diante do Partido Verde nos anos de 1980) foram rapidamente substituídas por tentativas de partidos tradicionais de avançar em suas abordagens diante das TICs modernas.

O papel da sociedade civil no contexto da filtragem na internet foca no que pode ser considerado funções clássicas de organizações da sociedade civil, sendo em maior parte a representação e defesa dos direitos dos cidadãos e a contribuição por especialistas. Em um contexto mais amplo de filtragem na internet (e outras formas de vigilância) existem aquelas organizações (em sua maioria ONGs mas também outras formas de grupos de experts) que incluem assuntos de internet em sua agenda já existente, como ONGs de direitos humanos e aquelas que foram formadas com um foco especial em políticas da internet. Nos casos de regimes de filtragem em países não democráticos há um amplo consenso entre organizações da sociedade civil que critica a censura e a perseguição de usuários da internet, bloggers ou jornalistas. O foco do debate está em definir uma resposta para a violação dos direitos básicos e dos direitos humanos (em especial a liberdade de expressão e a liberdade de imprensa). Ao mesmo tempo debates sobre a filtragem na internet em países democráticos assumem uma postura bem diferente. Não são as ONGs, mas sim grupos de experts que dominam o debate no setor da sociedade civil. Diferentemente de regimes autoritários, governos democráticos não ameaçam a integridade física dos usuários da internet, mas sim a liberdade da rede por si só (neutralidade de rede) e ao faze-lo estão limitando os direitos do usuário da internet. Os ativistas temem a introdução do regime de censura que tem inicio com um alvo amplamente aceito (pornografia infantil), mas posteriormente pode se expandir para conteúdos políticos e religiosos. E de fato, há uma grande possibilidade de políticas restritivas de filtragem na internet sejam expandidas a temas além do abuso de crianças, uma vez que essa infra-estrutura seja estabelecida. Além disso o problema de *overinclusiveness* é uma questão séria que encaminhará a censura de websites individuais automaticamente, como os casos de biblioteca dos EUA tem nos mostrado. O fato, que ao longo dos anos organizações da sociedade civil (especialmente aquelas com uma forte abordagem de política da internet) têm provado sua competência em relação às questões técnicas da internet, tem feito delas parceiras confiáveis e interessantes para os setores privados e públicos em países democráticos no caso de precisarem de assistência profissional ou até mesmo por razões de relações públicas. Por outro lado os atores da sociedade civil podem se tornar

grande oponentes especialmente para o setor público no caso de políticas restritivas de filtragem na internet.

O processo de governança da internet entre os anos de 1990 e 2010 tem sido dirigido por uma pluralidade de atores de todos os setores da sociedade. Ao comparar decisões diferentes ou processos políticos ao longo desses anos, torna-se claro que a inclusão de uma grande variedade de atores tem encaminhado a um ambiente mais estável para os processos de regulamentação. Isso pode ser visto pro exemplo no processo de constituição da ICANN, os processos do *Green Paper* e do *White Paper*, nos quais preocupações e descobertas de todos os atores eram colocados em pauta e discutidos para o desenvolvimento de uma solução baseada no compromisso mais compreensível possível. Em contraste, os esforços prévios de privatização da DNS aconteceram (basicamente por motives políticos) em ambientes mais exclusivos e fracassaram também devido a falta de apoio dos atores excluídos. Para evitar esses conflitos, o modelo de governança multisetorial se tornou um modelo de governança universalmente aceito pela comunidade de governança da internet. Um motivo maior para isso foi sua aplicação no Fórum de Governança da Internet que durante seu primeiro mandato de 2006 a 2010 conseguiu passar a idéia de multisetorialismo para atores de governança da internet em todas as partes do mundo que então aplicaram a idéia em seu contexto regional. Também os debates e conflitos nas áreas do cibercrime e filtragem na internet, como analisados nesta tese, se beneficiaram dessa abordagem. Por exemplo os debates sobre a filtragem especialmente na Europa e na América do Norte demonstraram que as tentativas individuais por parte do setor público de desenvolver políticas de internet causam não apenas o descontentamento, mas também podem resultar em falhas e danos técnicos ao funcionamento da internet em si. De qualquer maneira, apesar da abordagem multisetorial ter sido estabelecida como um modelo amplamente aceito, ela tem sido desafiada por numerosos governos que preferem desenvolver suas próprias políticas nacionais de Internet sem consultar as outras partes da sociedade. Os próximos anos, e também o desenvolvimentos durante o segundo mandato do IGF mostrarão se o modelo de governança multisetorial irá prevalecer e se o processo de governança da internet pode se tornar um modelo para processos de governança em outros domínios políticos.

Bibliografia

Adair, Steven: The Website for the President of Georgia Under Attack – Politically Motivated? Shadowserver Foundation, 20 July 2008. Available at: http://bit.ly/sfEX7p [Accessed 22 September 2009]

Ahlert, Christian: Democratic-Global-Governance.net. ICANN als Paradigma neuer Formen internationaler Politik, in: Internationale Politik und Gesellschaft, No 1, 2001, pp. 66-78. Available at: http://bit.ly/rH3kJf [Accessed 12 January 2010]

Ahmed, Shamima; Potter, David M.: NGOs in International Politics, Kumarian Press, Bloomfield, 2006

Akiner, Shirin: Violence in Andijan, Silk Road Paper, Central Asia - Caucasus Institute, Washington D.C., July 2005. Available at: http://bit.ly/vCFPUD [Accessed 07 October 2011]

Akkad, Omar el: Project Takes Aim at Internet Child Porn, The Globe and Mail, 24 November 2006. Available at: http://bit.ly/13xv45 [Accessed 13 May 2010]

Albright, David; Brannan, Paul; Walrond, Christina: Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Institute for Science and International Security, ISIS Report, Washington D.C., 22 December 2010. Available at: http://bit.ly/ezzUkT [Accessed 27 February 2011]

Allison, Juliann Emmons: Technology, Development, and Democracy. International Conflict and Cooperation in the Information Age, State University of New York Press, Albany, 2002

Amis, Lucy; Leisinger, Klaus M.; Schmitt, Karin: Human Rights and the Private Sector. International Symposium Report, Novartis Foundation for Sustainable Development, Zurich 2004. Available at: http://bit.ly/tGXCit [Accessed 07 July 2009]

Anderson, Ross; Clayton, Richard; Moore, Tyler: The Economics of Online Crime, in: The Journal of Economic Perspectives, Vol 23, No 3, Summer 2009, pp. 3-20

Anderson, Ross; Nagaraja, Shishir: The Snooping Dragon: SocialMalware Surveillance of the Tibetian Movement, Computer Laboratory, Technical Report No 746, University of Cambridge, March 2009. Available at: http://bit.ly/vikbGn [Accessed 22 September 2009]

Andrews, M.: Negative Caching of DNS Queries, RFC 2308, March 1998. Available at: http://bit.ly/uoiaao [Accessed 27 May 2009]

Antonova, Slavka: Power and Multistakeholderism in Internet Global Governance. Research Working Paper Series, Department of Management and International Business, Massey University, Auckland, 2007

Antonova, Slavka: Powerscape of Internet Governance, VDM Saarbrücken, 2008

APCERT: Annual Report 2010, APCERT Secretariat, 2011. Available at: http://bit.ly/rTHPaN [Accessed 21 October 2011]

APEC: Leaders Statement on Counter-terrorism, 21 October 2001. Available at: http://bit.ly/unNX4p [Accessed 11 September 2008]

APEC: Cybersecurity Strategy, Telecommunications and Information Working Group, 26th meeting, Moscow, 19-23 August 2002a. Available at: http://bit.ly/vjeCDs [Accessed 11 September 2008]

APEC: Shanghai Declaration, Shanghai, 29-30 May 2002b. Available at: http://bit.ly/ty279J [Accessed 11 September 2008]

APEC: Shanghai Declaration, Annex A: Program of Action, Shanghai 29-30 May 2002c. Available at: http://bit.ly/v1QLfF [Accessed 11 September 2008]

APEC: Shanghai Declaration, Annex B: Statement on the Security of Information and Communications Infrastructures, Shanghai 29-30 May 2002d. Available at: http://bit.ly/rMgpIy [Accessed 11 September 2008]

Arkin, William: The Cyber Bomb in Yugoslavia, Washington Post, 25 October 1999. Available at: http://wapo.st/tbkJrK [Accessed 22 September 2009]

Asseburg, Muriel: Der Arabische Frühling. Herausforderung und Chance für die deutsche und europäische Politik, SWP-Studie, Stiftung Wissenschaft und Politik, Berlin, Juli 2011. Available at: http://bit.ly/rss59P [Accessed 19 August 2011]

Back, Aaron: China Pulls Back from Edict on Web-Filtering Software, The Wall Street Journal, 14 August 2009. Available at: http://on.wsj.com/wISbc [Accessed 16 March 2010]
Bandurski, David: China's Guerrilla War for the Web, Far Eastern Economic Review, July 2008. Available at: http://bit.ly/v4P4Xg [Accessed 22 May 2009]

Banerjee, Indrajit: The Internet and Governance in Asia, Nanyang Technology University, Singapore, 2007

Baran, Paul: On Distributed Communications, RAND Corporation, August 1964. Available at: http://bit.ly/gh4Qs7 [Accessed 11 September 2008]

Baran, Paul: On Distributed Communications Networks, RAND Corporation, September 1962. Available at: http://bit.ly/oo5n20 [Accessed 11 September 2008]

Barnett, Michael; Duvall, Raymond: Power in Global Governance, Cambridge University Press, Cambridge, 2005

Bastian, Jeannette Allis: Filtering the Internet in American Public Libraries: Sliding Down the Slippery Slope, First Monday, Vol 2, No 10, 6 October 1997. Available at: http://bit.ly/rYdduS [Accessed 25 May 2009]

Batliwala, Srilatha; Brown, L. David: Transnational Civil Society, Kumarian Press, Bloomfield, 2006

BBC: Google Censors Itself for China. 25 January 2006. Available at: http://bbc.in/18jjcE [Accessed 13 July 2009]

BBC: Yahoo 'Helped Jail China Writer'. 7 September 2005. Available at: http://news.bbc.co.uk/2/hi/asia-pacific/4221538.stm [Accessed 13 July 2009]

Beck, Ulrich: Risikogesellschaft. Auf dem Weg in eine andere Moderne, Suhrkamp, Frankfurt/M, 1986

Beck, Ulrich: Weltrisikogesellschaft, Suhrkamp, Frankfurt/M, 2008

Bendrath, Ralf: Global Technology Trends and National Regulation: Explaining Variation in the Governance of Deep Packet Inspection, Delft University of Technology, 2009. Available at: http://bit.ly/uERGzx [Accessed 22 September 2010]

Benedek, Wolfgang; Bauer, Veronika; Kettemann, Matthias C.: Internet Governance and the Information Society: Global Perspectives and European Dimensions, Boom Eleven International, Den Haag, 2008

Berg, Stefan; Rosenbach, Marcel: Schwarz-Gelb rückt von Internetsperren ab, Spiegel Online, 08 February 2010. Available at: http://bit.ly/bCdmaE [Accessed 15 November 2010]

Biermann, Kai: Aktionismus hilft nicht gegen Kinderpornos, Zeit Online, 05 March 2009a. Available at: http://bit.ly/10cV34 [Accessed 13 March 2010]

Biermann, Kai: Keine Allmacht für das BKA, Zeit Online, 14 May 2009b. Available at: http://bit.ly/uERGzx [Accessed 13 March 2010]

Biermann, Kai: Missbrauchsopfer gegen Netzsperren, Zeit Online, 13 June 2009c. Available at: http://bit.ly/AksXXV [Accessed 13 March 2010]

Blank, Stephen: The Strategic Importance of Central Asia: An American View, Parameters, Spring 2008, pp. 73-87. Available at: http://bit.ly/uqDWtB [Accessed 24 March 2009]

Bleich, Holger; Kossel, Axel: Verschleierungstaktik. Die Argumente für Kinderporno-Sperren laufen ins Leere, c't Magazin, 9/09, 2009. Available at: http://bit.ly/c6PuQy [Accessed 11 June 2010]

Borgen, Christopher J.: Imagining Sovereignty, Managing Secession: The Legal Geography of Eurasia's "Frozen Conflicts", Legal Studies Research Paper Series, Paper #090168, St John's University School of Law, February 2009. Available at: http://bit.ly/uERGzx [Accessed 22 September 2009]

Borger, Julian; Dehghan, Saeed Kamali: Attack in Iranian Scientists Prompts Hit Squad Claim, The Guardian, 29 November 2010. Available at: http://bit.ly/ff1cfG [Accessed 15 December 2010]

Boston Working Group (BWG): The Boston Meeting Consensus For Changes To The IANA/NSI Draft By-Laws, n.d. Available at: http://1.usa.gov/vSIyh6 [Accessed 05 June 2009]

Boyd, Clark: Romania tackles rise in cyber-crime, BBC, 27 December 2003. Available at: http://bbc.in/sbKjL4 [Accessed 16 March 2008]

Brenner, Susan W.: Cybercrime: Criminal Threats From Cyberspace, Praeger, Santa Barbara, 2010

Brenner, Susan W.: Interview on 4 March 2011. Available at: http://bit.ly/sjy4NS

Bright, Martin: BT Puts Block on Child Porn Sites, The Guardian, 6 June 2004. Available at: http://bit.ly/rPsSsJ [Accessed 26 June 2009]

Bristow, Michael: China Defends Screening Software, BBC, 9 June 2009. Available at: http://bbc.in/mLzSx [Accessed 15 October 2009]

Broder, John M.: Ira Magaziner Argues for Minimal Internet Regulation, New York Times, 30 June 1997. Available at: http://nyti.ms/wApIMI [Accessed 23 June 2009]

Castells, Manuel: The Internet Galaxy, Oxford University Press, Oxford, 2001

Cave, Jonathan et al: Responsibility in the Global Information Society. Towards Multi-stakeholder Governance, RAND Europe, British Telecommunications, 2007. Available at: http://bit.ly/tXrylw [Accessed 22 November 2010]

Center for Democracy and Technology (CDT): Comments regarding: The Continued Transition of the Technical Coordination and Management of the Internet's Domain Name and Addressing System: Midterm Review of the Joint Project Agreement, 25 January 2008. Available at: http://1.usa.gov/vJmNv4 [Accessed 05 June 2009]

Cerf, V.: I remember IANA, RFC 2468, 17 October 1998. Available at: http://bit.ly/2s5cmH [Accessed 20 April 2010]

Cerf, Vinton G.; Kahn, Robert E.: A Protocol for Packet Network Intercommunication, IEEE Trans on Comms, Vol Com-22, No 5, May 1974. Available at: http://bit.ly/rMSdk0 [Accessed 22 June 2010]

CGG: Our Global Neighborhood. The Report of the Commission on Global Governance. Oxford University Press, Oxford 1995

Chabrow, Eric: Cyber Attacks: How Worried Should We Be? Holiday Hackers Victimize White House, Pentagon, NYSE Sites, GovInfo Security, 9 July 2009. Available at: http://bit.ly/11FMpM [Accessed 22 September 2009]

Chacksfield, Marc: The Pirate Bay Once Again Blocked in Denmark, Techradar.com, 20 January 2009. Available at: http://bit.ly/t0Jrcd [Accessed 07 October 2011]

Chen, Thomas M.; Robert, Jean-Marc: The Evolution of Viruses and Worms, in: Chen, William

W.S.: Statistical Methods in Computer Security, CRC Press, London, 2004, pp. 265-286

Cheng, Kenneth H.;Bandyopadhyay, Subhajyoti; Guo, Hong: The Debate on Net Neutrality: A Policy Perspective, Information Systems Research, Forthcoming, 25 June 2008. Available at: http://bit.ly/rwz366 [Accessed 22 September 2009]

Chip Online: Bundestag beschließt Netzsperren-Gesetz, 19 June 2009. Available at: http://bit.ly/t33uSo [Accessed 25 April 2010]

Choo, Kim-Kwang Raymond: Organised Crime Groups in Cyberspace: A Typology, Trends in Organized Crime, Vol 11, No 3, 2008, pp. 270-295

Chowdhury, Mridul: The Role of the Internet in Burma's Saffron Revolution, Internet & Democracy Case Study Series, Berkman Center for Internet and Society, September 2008. Available at: http://bit.ly/vZmIQe [Accessed 27 May 2009]

Clark, David D.: Name, Addresses, Ports, and Routes, RFC 814, July 1982. Available at: http://bit.ly/vCdnyk [Accessed 20 April 2010]

Clinton, David; Morgenthau, Hans J.; Thompson, Kenneth W.: Politics Among Nations. Mcgraw Hill Book, Columbus 2005 (orig. 1948)

Closson, Stacy; Halbach, Uwe: Die Georgienkrise in ihrer kaukasischen Dimension, SWP-Aktuell 75, Stiftung Wissenschaft und Politik, Berlin, Oktober 2008. Available at: http://bit.ly/tmCfzB [Accessed 22 September 2009]

Clover, Charles: Kremlin-Backed Group Behind Estonia Cyber Blitz, Financial Times, 11 March 2009. Available at: http://on.ft.com/sRb7vl [Accessed 22 September 2009]

CNET News: U.S. Rejects Net Name Plan, 2 May 1997. Available at: http://cnet.co/sBItmH [Accessed 16 May 2009]

CNNIC: 18th Statistical Survey Report on the Internet Development in China, July 2006. Available at: http://bit.ly/uGn2Io [Accessed 22 March 2011]

CNNIC: CNNIC Releases 2007 Survey Report on China Weblog Market. Number of Blog Writers Reaches 47 Million Equaling One Fourth of Total Netizens, 27 December 2007. Available at: http://bit.ly/kLu3nE [Accessed 25 March 2008]

CNNIC: Statistical Report on Internet Development in China, July 2010. Available at: http://bit.ly/b06eD7 [Accessed 22 March 2011]

Collins, John: Eircom to Block Internet Access to Pirate Bay as Other Firms Refuse, Irish Times, 8 Augusts 2009. Available at: http://bit.ly/nDFof [Accessed 02 April 2010]

Commission of the European Communities: Critical Infrastructure Protection in the Fight Against Terrorism, COM (2004) 702 final, Brussels, 20 October 2004. Available at: http://bit.ly/vu1Kr0 [Accessed 15 May 2008]

Commonwealth of Nations: Commonwealth Cybercrime Initiative, Proposal, 19 July 2011. Available at: http://bit.ly/vOWRig [Accessed 19 June 2010]

Commonwealth of Nations: Model Law on Computer and Computer Related Crime, LMM(02)17, London, October 2002. Available at: http://bit.ly/vJcpMW [Accessed 19 June 2010]

Constantin, Lucian: The Embassy of Portugal in India Falls Victim To Hackers, Softpedia.com, 21 March 2009a. Available at: http://bit.ly/vzb6dP [Accessed 22 September 2009]

Constantin, Lucian: Websites of Three More Embassies Spreading Malware, Softpedia.com, 17 March 2009b. Available at: http://bit.ly/9YxVWv [Accessed 22 September 2009]

Cook, Sarah: China’s Growing Army of Paid Internet Commentators, Freedom House, 11 October 2011. Available at: http://bit.ly/qJVl0N [Accessed 13 October 2011]

Corbin, Kenneth: Lessons From The Georgia-Russia Cyberwar, Institute of Communication Studies, University of Leeds, 12 March 2009. Available at: http://bit.ly/uPWqam [Accessed 22 September 2009]

Cordesman, Anthony H.: The Saudi Arms Sale, Center for Strategic and International Studies, Washington D.C., 3 November 2010. Available at: http://bit.ly/hvctqI [Accessed 12 April 2011]

Cornell, Svante E.: Geopolitics and Strategic Alignments in the Caucasus and Central Asia, Perceptions: Journal of International Affairs, Vol. IV, No 2, June-August 1999. Available at: http://bit.ly/vz0v59 [Accessed 07 October 2011]

Cornish, Paul: Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks, European Parliament, Policy Department External Policies, February 2009. Available at: http://bit.ly/tOhzFZ [Accessed 22 September 2009]

Costello, A.: Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA), RFC 3492, March 2003. Available at: http://bit.ly/uocjPV [Accessed 27 May 2009]

Council of Europe (CoE): Additional Protocol to the Convention on Cybercrime, CETS No.: 189, Strasbourg, 28 January 2003. Available at: http://bit.ly/ttlPel [Accessed 15 September 2008]

Council of Europe (CoE): Convention on Cybercrime, CETS No.: 185, Budapest, 23 November 2001. Available at: http://bit.ly/ja41X2 [Accessed 15 September 2008]

Council of Europe (CoE): Project on Cybercrime in Georgia, Policy Advice (DGHL/2009/2215), 19 May 2009. Available at: http://bit.ly/snHUHT [Accessed 11 March 2010]

Council of the European Union: Council Framework Decision on Attacks against Information Systems, 2005/222/JHA, 24 February 2005. Available at: http://bit.ly/tQmkDM [Accessed 27 May 2009]

Council of the European Union: Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime, 2001. Available at: http://bit.ly/vEZEo1 [Accessed 27 May 2009]

Davies, D.W. et al: A Digital Communication Network for Computers Giving Rapid Response at Remote Terminals, National Physical Laboratory, Teddington, Middlesex, n.d. Available at: http://bit.ly/w4KtzT [Accessed 23 May 2008]

Davis, Joshua: Hackers Take Down the Most Wired Country in Europe, Wired Magazien, Issue 15.09, 21 August 2007. Available at: http://bit.ly/cyafj0 [Accessed 22 September 2009]

Deering, S.; Hinden, R.: Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December 1998. Available at: http://bit.ly/jAa9h2 [Accessed 27 May 2009]

Deibert, Ron; Rohozinski, Rafal: Tracking GhostNet: Investigating a Cyber Espionage Network, Information Warfare Monitor, March 2009, Toronto. Available at: http://scr.bi/tC3clh [Accessed 22 September 2009]

Deibert, Ronald; Palfrey, John; Rohozinski, Rafal; Zittrain, Jonathan: Access Denied. The Practice and Policy of Global Internet Filtering. MIT Press, Cambridge 2008

Deibert, Ronald; Palfrey, John; Rohozinski, Rafal; Zittrain, Jonathan: Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace, MIT Press, Cambridge, 2010

DeNardis, Laura: Protocol Politics. The Globalization of Internet Governance, MIT Press, Cambridge, 2009

Department of Commerce (DOC), National Telecommunications and Information Administration (NTIA), Improvement of Technical Management of

Internet Names and Addresses; Proposed Rule, Federal Register, Docket No. 980212036–8036–01, Vol 63, No 34, 20 February 1998a. Available at: http://1.usa.gov/rwjgWn [Accessed 05 June 2009]

Department of Commerce (DOC), National Telecommunications and Information Administration (NTIA), Letter by Jake Winebaum to NTIA, 20 March 1998b. Available at: http://1.usa.gov/vDkMYC [Accessed 05 June 2009]

Department of Commerce (DOC), National Telecommunications and Information Administration (NTIA), Letter by Michelena Hallie and Anne Lucey to NTIA, 23 March 1998c. Available at: http://1.usa.gov/v4wovb [Accessed 05 June 2009]

Department of Commerce (DOC), National Telecommunications and Information Administration (NTIA), Letter by William W. Burrington to NTIA, 23 March 1998d. Available at: http://1.usa.gov/sBcaui [Accessed 05 June 2009]

Deutscher Bundestag: Petition: Internet - Keine Indizierung und Sperrung von Internetseiten, 22 April 2009. Available at: http://bit.ly/vL2dm [Accessed 19 July 2010]

Dingledine, Roger; Mathewson, Nick; Syverson, Paul: Proceedings of the 13th USENIX Security Symposium, USENIX Association, San Diego, 9-13 August 2004. Available at: http://bit.ly/ty8Ctj [Accessed 24 March 2008]

Dingwerth, Klaus; Pattberg, Philipp: Was ist Global Governance? In: Leviathan. Berliner Zeitschrift für Sozialwissenschaften 34 (3), 377-399, Berlin 2006

Dixon, Laura; Ahmed, Murad: Russia and China Accused of Harbouring Cybercriminals, The Times, 09 December 2008. Available at: http://thetim.es/sxnwVq [Accessed 14 September 2009]

Donnerhacke, Lutz: Von der Leyens unseriöse Argumentation, Zeit Online, 20 May 2009. Available at: http://bit.ly/ii3m7 [Accessed 17 October 2009]

Doria, Avri; Kleinwächter, Wolfgang: Internet Governance Forum (IGF). The First Two Years, IGF Secretariat, 2008. Available at: http://bit.ly/ufCcQP [Accessed 05 June 2009]

Dornseif, Maximillian: Government Mandated Blocking of Foreign Web Content, in: Knop, Jan von; Haverkamp, Wilhelm; Jessen, Eike: Security, E-Learning, E-Services: Proceedings of the 17. DFN-Arbeitstagung über Kommunikationsnetze, Düsseldorf, 2003, pp. 617-648. Available at: http://bit.ly/rxhBuL [Accessed 25 July 2010]

Drake, Bill: Interview on 6 May 2011. Available at: http://bit.ly/sXkjdf

Drummond, David: A New Approach to China: An Update, The Official Google Blog, 22 March 2010. Available at: http://bit.ly/cjGcqR [Accessed 13 August 2010]

Dunn, Myriam A.: The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue With Assistance of the Morphological Method. In: Information and Security, Vol 7, 2001, pp 145-158. Available at: Available at: http://bit.ly/tZOoUE [Accessed 22 September 2009] [Accessed 22 September 2009]

eco: Russland ist Musterschüler beim Kampf gegen Internet-Kinderpornographie, Pressemeldung, Verband der deutschen Internetwirtschaft e.V., 08 November 2010. Available at: http://bit.ly/uzIF2M [Accessed 30 March 2011]

Eijk, Nico van; Maniadaki, Katerina: Institutional Aspects of Internet Governance, in: Möller, Christian; Amouroux, Arnaud: Governing the Internet - Freedom and Regulation in the OSCE Region, OSCE, Vienna, 2007, pp. 67-87

European Commission: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890 final, Brussels, 26 January 2001. Available at: http://bit.ly/w56TJS [Accessed 19 March 2010]

European Commission: Proposal for a Directive on Attacks against Information Systems and Repealing Council Framework Decision 2005/222/JHA, COM(2010) 517, Brussels, 2010a. Available at: http://bit.ly/vchR75 [Accessed 19 March 2010]

European Commission: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM(2010) 673 final, Brussels, 22 November 2010b. Available at: http://bit.ly/rPSzaT [Accessed 19 March 2010]

European Commission: Towards a General Policy on the Fight against Cyber Crime, COM(2007) 267 final, Brussles, 22 May 2007. Available at: http://bit.ly/vrfw3G [Accessed 19 March 2010]

Everard, Jerry: Virtual States. The Internet and the Boundaries of the Nation-State, Routledge, London, 2000

Faltstrom, P.; Hoffman, P.: Internationalizing Domain Names in Applications (IDNA), RFC 3490, March 2003. Available at: http://bit.ly/uptGzo [Accessed 27 May 2009]

Fareed, Malik: China Joins a Turf War, The Guardian, 22 September 2008. Available at: http://bit.ly/33RMda [Accessed 17 November 2008]

Faris, Robert; Roberts, Hal; Wang, Stephanie: China's Green Dam, The Implications of Government Control Encroaching on the Home PC, OpenNet Initiative, ONI Bulletin, 2009. Available at: http://bit.ly/vDoTCf [Accessed 22 June 2010]

Faz.net: Ist Ein Internetangriff der Ernstfall? 18 June 2007. Available at: http://bit.ly/vAkhwl [Accessed 22 September 2009]

Federrath, Hannes: Öffentliches Expertengespräch des Unterausschusses Neue Medien des Ausschusses für Kultur und Medien des Deutschen Bundestages zu den rechtlichen und technischen Möglichkeiten und Grenzen von Sperrungsverfügungen kinderpornographischer Inhalte im Internet, Berlin, 12 February 2009. Available at: http://bit.ly/vOraUG [Accessed 16 March 2010]

Filiol, Eric: Computer Viruses: From Theory to Applications, Springer, Berlin, 2005

Financial Action Task Force (FATF): FATF 40 Recommendations, October 2003. Available at: http://bit.ly/sOdnh7 [Accessed 25 March 2009]

Financial Action Task Force (FATF): Vulnerabilities of Casinos and Gaming Sector, March 2009. Available at: http://bit.ly/9P73jS [Accessed 25 March 2010]

Fischer, Sebastian; Medick, Veit; Peters, Dominik: Politiker lassen ihre Häuser pixeln, Spiegel Online, 12 August 2010, Available at: http://bit.ly/aKd0cL [Accessed 15 August 2011]

Focus Online: Wirksamkeit von Kinderporno-Sperrungen umstritten, 28 March 2009. Available at: http://bit.ly/Wn4c [Accessed 15 July 2009]

Fossato, Floriana; Lloyd, John; Verkhofsky, Alexander: The Web That Failed, Reuters Institute for the Study of Journalism, University of Oxford, 2008. Available at: http://bit.ly/H0wGC [Accessed 22 September 2009]

Fossi, Marc: Symantec Global Internet Security Threat Report: Trends for 2009, Vol XV, April 2010. Available at: http://bit.ly/dBVktQ [Accessed 15 September 2010]

Franda, Marcus: Governing the Internet. The Emergence of an International Regime, Lynne Rienner Publishers, London, 2001

Freedom House: China and the Internet. An Uphill Fight for Freedom, Harvard International Review, 26 October 2009. Available at: http://bit.ly/9fwwPe [Accessed 22 May 2010]

Froomkin, A. Michael: Almost Free: An Analysis of ICANN's 'Affirmation of Commitments', Journal on Telecommunications and Hight Technology Law, Vol 9, Issue 1, Winter 2011, pp. 187-233. Available at: http://bit.ly/gURSUA [Accessed 05 June 2009]

Froomkin, A. Michael: ICANN's "Uniform Dispute Resolution Policy" - Causes and (Partial) Cures, Brooklyn Law Review, Vol 67, No 3, 2002. Available at: http://bit.ly/pAvHU6 [Accessed 05 June 2009]

Froomkin, A. Michael: Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution, Duke Law Journal, Vol 50, No 17, 2000, pp. 17-184. Available at: http://bit.ly/vdl8iX [Accessed 05 June 2009]

Fues, Thomas; Hamm, Brigitte I.: Die Weltkonferenzen der 90er Jahre: Baustellen für Global Governance, Dietz, Bonn, 2001

G8: Communique, Meeting of Justice and Interior Ministers of the Eight, Washington D.C., 9-10 December 1997. Available at: http://bit.ly/rFbD46 [Accessed 12 December 2009]

G8: Communique, Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, 19-20 October 1999, Moscow. Available at: http://1.usa.gov/tPOEBd [Accessed 12 December 2009]

G8: Justice and Home Affairs Communique, Washington D.C., 11 May 2004. Available at: http://bit.ly/rEXuo6 [Accessed 12 December 2009]

G8: Ministers of Justice and Interior, Press Conference on the Results of the G8 Justice and Home Affairs Ministerial, Moscow, 16 June 2006. Available at: http://bit.ly/rS57W1 [Accessed 12 December 2009]

G8: Recommendations on Transnational Crime, 2002. Available at: http://bit.ly/uGZK7r [Accessed 23 November 2008]

Gardner, Frank: Saudia Arabia Awaits Internet Connection, BBC, 12 October 1998. Available at: http://bbc.in/tnpn3H [Accessed 15 September 2008]

George, Alexander L.; Bennet, Andrew: Case Studies and Theory Development in the Social Sciences, MIT Press, Cambridge, 2005

Gercke, Marco: Interview on 9 March 2011. Available at: http://bit.ly/ttT5K6

Gerring, John: What Is A Case Study And What Is It Good For? American Political Science Review, Vol 98 No 2, May 2004

Giacomello, Giampiero: National Governments and Control of the Internet, Routledge, New York, 2005

Global Network Initiative: Principles on Freedom of Expression and Privacy. Available at: http://bit.ly/8y59IV [Accessed 18 July 2009]

Goldsmith, Jack; Wu, Tim: Who Controls the Internet? Oxford University Press, New York, 2006

Goodwin, Jacob: Russian “Hacktivists“ Used Turkish Botnets to Attack Georgia, Government Security News Magazine, 23 September 2008. Available at: http://bit.ly/u6kugk [Accessed 22 September 2009]

Gorman, Siobhan: Electricity Grid in U.S. Penetrated by Spies, Wall Street Journal, 8 April 2009. Available at: http://on.wsj.com/fhGdG [Accessed 22 September 2009]

Grant, Ian: Kaspersky reveals price list for botnet attacks, ComputerWeekly.com, 23 July 2009. Available at: http://bit.ly/uXM7NL [Accessed 22 September 2009]

Grossman, Lawrence: Electronic Republic: Reshaping American Democracy for the Information Age, Penguin, New York, 1996

Güntner, Joachim: German Angst, NZZ Online, 29 March 2011. Available at: http://bit.ly/fbvsNT [Accessed 20 August 2011]

Halliday, Fred: The Romance of Non-State Actors, in: Josselin, Daphne; Wallace, William: Non-State Actors in World Politics, Palgrave, New York, 2001, pp. 21-37

Hansen, Lene; Nissenbaum, Helen: Digital Disaster, Cyber Security, and the Copenhagen School, in: International Studies Quarterly, Vol 53, No 4, December 2009, pp. 1155-1175

Hauck, Mirjam: "Zensur wird salonfähig", Sueddeutsche.de, 25 March 2009. Available at: http://bit.ly/vWKokw [Accessed 17 January 2010]

Haufler, Virginia: New Forms of Governance: Certification Regimes as Social Regulations of the Global Market, in: Meidinger, Errol; Elliott, Chris; Oesten, Gerhard: Social and Political Dimensions of Forest Certification, Forstbuch.de, 2003, pp. 237-247. Available at: http://bit.ly/ug02hE [Accessed 22 July 2009]

Hebestreit, Steffen: Löschen statt Sperren funktioniert, Frankfurter Rundschau, 21 January 2011. Available at: http://bit.ly/u85Ivx [Accessed 13 July 2011]
Held, David; McGrew, Anthony: Governing Globalization, Polity Press, Cambridge, 2005

Held, David; McGrew, Anthony: The Global Transformations Reader, Polity Press, Cambridge, 2003

Heller, Regine: Die russische Jugendbewegung "Naschi". Aufstieg und Fall eines polit-technologischen Projekts in der Era Putin, in: Russland-Analysen Nr 168, Deutsche Gesellschaft für Osteueropakunde, 11 July 2008, pp. 2-4. Available at: http://bit.ly/rqpXyQ [Accessed 22 September 2009]

Hemmati, Minu: Multi-Stakeholder Processes for Governance and Sustainability, Earthscan, London 2002

Higgins, Marc: Symantec Internet Security Threat Report, Attack Trends for Q3 and Q4 2002, Report Vol 3, February 2003

Hunter, Christopher D.: Internet Filter Effectiveness: Testing Over and Underinclusive Blocking Decisions of Four Popular Filters, in: Social Science Computer Review, Vol 18, No 2, June 2000. Available at: http://bit.ly/sUrCy8 [Accessed 15 March 2009]

Hocking, Brian: Basics of Multistakeholder Diplomacy, in: Kurbalija, Jovan; Katrandjiev, Valentin: Multistakeholder Diplomacy. Challenges and Opportunities, Diplo Foundation, Malta, 2006. Available at: http://bit.ly/t0GzSZ [Accessed 10 September 2010]

Hoffmann, Bert: The Politics of the Internet in Third World Development: Challenges in Contrasting Regimes with Case Studies of Costa Rica and Cuba, Routledge, London, 2004

ICANN: Amendment 11 to Cooperative Agreement Between NSI and U.S. Government, 7 October 1998a. Available at: http://bit.ly/sVtMAT [Accessed 05 June 2009]

ICANN: Annual Report 2008. Available at: http://bit.ly/f0SBrL [Accessed 05 June 2009]

ICANN: Contract Between ICANN and the United States Government for Performance of the IANA Function, 8 February 2000. Available at: http://bit.ly/t8nHVN [Accessed 05 June 2009]

ICANN: Final Implementation Plan for IDN ccTLD Fast Track Process, 16 November 2009. Available at: http://bit.ly/uOpOEJ [Accessed 22 January 2010]

ICANN: First Four Internationalized Domain Names Pass Key Approval Milestone, ICANN News Release, 21 January 2010a. Available at: http://bit.ly/6h4Qg8 [Accessed 17 February 2010]

ICANN: ICANN Approves Chinese Internationalized Domain Names, ICANN News Release, 25 June 2010b. Available at: http://bit.ly/ddUNfV [Accessed 25 August 2010]

ICANN: ICANN-NSI Registry Agreement, 04 November 1999. Available at: http://bit.ly/vAXG7H [Accessed 05 June 2009]

ICANN: IDN ccTLD Fast Track String Evaluation Completion. Available at: http://bit.ly/4Fso2T [Accessed 18 January 2011]

ICANN: Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers, November 1998b. Available at: http://bit.ly/cQd0mf [Accessed 05 June 2009]

ICANN Bylaws: Bylaws for Internet Corporation for Assigned Names and Numbers, Article 1, Section 1. Available at: http://bit.ly/vHVJGY [Accessed 05 June 2009]

Ikenberry, G. John: The Rise of China and the Future of the West, Foreign Affairs, Vol 87, No 1, January/February 2008.

International Ad Hoc Committee (IAHC): Final Report of the International Ad Hoc Committee: Recommendations for Administration and Management of gTLDs, 4 February 1997. Available at: http://bit.ly/jEPRSA [Accessed 14 May 2009]

International Chamber of Commerce (ICC): ICC views on the mid-term review of the Joint Project Agreement between ICANN and the US Department of Commerce, Commission on E-Business, IT and Telecoms, Task Force on Internet and Telecoms Infrastructure and Services (ITIS), 6 February 2008. Available at: http://1.usa.gov/u2izhE [Accessed 05 June 2009]

International Telecommunication Union (ITU): Global Cybersecurity Agenda, 2007. Available at: http://bit.ly/9gXxhC [Accessed 25 March 2009]

International Telecommunication Union (ITU): Global Strategic Report, Global Cybersecurity Agenda, High-Level Experts Group, 2008. Available at: http://bit.ly/scyrZa [Accessed 25 March 2009]

International Telecommunication Union (ITU): ITU Toolkit for Cybercrime Legislation, February 2010. Available at: http://bit.ly/TC2ND [Accessed 25 March 2009]

Internet Governance Project (IGP): Comments on: The Continued Transition of the Technical Coordination and Management of the Internet's Domain Name and Addressing System: Midterm Review of the Joint Project Agreement, 15 February 2008. Available at: http://1.usa.gov/tTuzHM [Accessed 05 June 2009]

Internet Watch Foundation (IWF): Annual and Charity Report 2008, Cambridge, 2009. Available at: http://bit.ly/uVzND6 [Accessed 17 May 2010]

Internet World Stats: http://www.internetworldstats.com

ITU Internet Statistics 2008. Available at: http://bit.ly/tfQtcS [Accessed 22 September 2009]

Jarvik, Laurence: Shirin Akiner on the Andijan Controversy, Registan.net, 18 September 2005. Available at: http://bit.ly/vkQRfZ [Accessed 13 July 2010]

Johnson, Bobbie: Amnesty Criticises Global Network Initiative for Online Freedom of Speech. Guardian.co.uk, 30 October 2008. Available at: http://bit.ly/4yYEka [Accessed 13 July 2009]

Johnson, Mike: Georgian Websites Under Attack – Don't Believe the Hype. Shadowserver Foundation, 12 August 2008. Available at: http://bit.ly/tMsfpR [Accessed 22 September 2009]

Kahin, Brian; Keller, James H.: Coordinating the Internet, MIT Press, Cambridge, 1997

Kalathil, Shanthi; Boas, Taylor C.: Open Networks, Closed Regimes. The Impact of the Internet on Authoritarian Rule, Carnegie Endowment for International Peace, Brookings Institution Press, Washington D.C., 2003

Karns, Margaret P.; Mingst, Karen A.: International Oragnizations. The Politics and Processes of Global Governance. Lynne Rienner Publishers, Boulder 2004

Kell, Georg; Ruggie, John Gerard: Global markets and social legitimacy: the case for the 'Global Compact', Transnational Corporations, Vol 8, No 3, December 1999, pp. 101-120. Available at: http://bit.ly/w2nsKy [Accessed 12 May 2008]

Keohane, Robert O.; Nye, Joseph S.: Power and Interdependence, Longman, New York, 2001

Kerr, Kathryn: Putting Cyberterrorim into Context, AusCERT, 24 October 2003

Available at: http://bit.ly/rBtHGw [Accessed 22 September 2009]

Kirk, Jeremy: Georgia Cyberattacks Linked to Russian Organized Crime, PC World, 17 August 2009. Available at: http://bit.ly/17ViOM [Accessed 22 September 2009]

Kirk, Jeremy: Student Fined For Attack On Estonian Website, InfoWorld, 24 January 2008. Available at: http://bit.ly/rNs5Ih [Accessed 22 September 2009]

Kiss, Jemima: Why everyone's a winner, The Guardian, 10 November 2008. Available at: http://bit.ly/olnGli [Accessed 05 June 2009]

Klein, Hans: ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy, The Information Society, 18, 2002, pp. 193-207. Available at: http://bit.ly/rOQwe2 [Accessed 05 June 2009]

Kleinwächter, Wolfgang: Interview on 7 July 2011. Available at: http://bit.ly/vX9kJD

Kleinwächter, Wolfgang: The Power of Ideas. Internet Governance in a Global Multi-Stakeholder Environment, Marketing für Deutschland GmbH, Berlin, 2007

Kleinrock, Leonard: Communication Nets: Stochastic Message Flow and Delay, Dover Publications, Mineloa, 2007

Kleinrock, Leonard: History of the Internet and its Flexible Future, IEEE Wireless Communication, February 2008. Available at: http://scr.bi/sYzMoh [Accessed 15 September 2008]

Klingebiel, Stephan; Roehder, Katja: The Development-Military Relationship: the Start of a New Alliance? German Development Institute, Briefing Paper 1/2004. Available at: http://bit.ly/unX5eZ [Accessed 07 July 2009]

Knake, Robert K.: Internet Governance in an Age of Cyber Insecurity, Council Special Report No 56, Council on Foreign Relations, Washington D.C., September 2010. Available at: http://on.cfr.org/szZTYS [Accessed 11 November 2010]

Knight, Gavin: Kremlin Eyes Internet Control, The Guardian, 3 January 2008. Available at: http://bit.ly/vAGvXt [Accessed 22 March 2009]

König, Marietta S.: Not Frozen But Red Hot: Conflict Resolution in Georgia Following the Change of Government, in: OSCE Yearbook 2006, Centre for OSCE Research, Hamburg 2006. Available at: http://bit.ly/uYOclu [Accessed 22 September 2009]

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität (KOBIK): Jahresbericht 2009. Available at: http://bit.ly/tVNve7 [Accessed 14 March 2011]

Koppel, Andrea: China places roadblocks on the Internet, CNN, 9 February 1996. Available at: http://bit.ly/u3Anqi [Accessed 04 April 2009]

Krasner, Stephen: International Regimes. Cornell University Press. Ithaka 1984

Krempl, Stefan: Ausweitung der Web-Sperren auf Hasspropaganda gefordert, Heise Online, 9 July 2009a. Available at: http://bit.ly/12PyTb [Accessed 18 July 2009]

Krempl, Stefan: Bundeskabinett beschließt Gesetzesentwurf zu Kinderporno-Sperren, Heise Online, 22 April 2009b. Available at: http://bit.ly/eu01nm [Accessed 20 July 2009]

Krempl, Stefan: CDU-Rechtspolitiker will Internetsperren gegen Urheberrechtsverletzer, Heise Online, 26 September 2011. Available at: http://bit.ly/oJwisq [Accessed 29 September 2011]

Krempl, Stefan: Fünf Provider unterzeichnen Vertrag zu Kinderporno-Sperren, Heise Online, 17 April 2009c. Available at: http://bit.ly/u6sdNo [Accessed 12 March 2011]

Krempl, Stefan: Internet-Sperren vorerst vom Tisch, c't Magazin, 23/09, 2009d. Available at: http://bit.ly/uXCLG2 [Accessed 16 July 2010]

Krempl, Stefan: Keine Internetsperren bei Urheberrechtsverstößen, Heise Online, 30 January 2009e. Available at: http://bit.ly/vBo5GP [Accessed 29 September 2011]

Krempl, Stefan: Provider in Nordrhein-Westfalen erhalten Sperrungsverfügungen, Heise Online, 08 February 2002. Available at: http://bit.ly/tQfI02[Accessed 05 June 2009]

Kurbalija, Jovan; Katrandjiev, Valentin: Multistakeholder Diplomacy. Challenges and Opportunities. Diplo Foundation, Malta 2006

Lang, Kai-Olaf: Die baltischen Staaten und ihr schwieriges Verhältnis zu Russland, SWP-Aktuell 2008/A 61, July 2008. Available at: http://bit.ly/ykQmG0 [Accessed 25 May 2010]

Lawson, Stephen: Update: ICANN assigns its last IPv4 addresses, InfoWorld, 03 February 2011. Available at: http://bit.ly/h0PrHm [Accessed 05 June 2009]

Leiner et al: The Past and Future History of the Internet, Communications of the ACM, Vol 40, No 2, February 1997, pp. 102-108. Available at: http://bit.ly/tK77aP [Accessed 02 May 2008]

Lemos, Ronaldo et al: Tecnobrega: O Pará Reinventando o Negócio da Música, Fundação Getulio Vargas, Rio de Janeiro, 14 July 2008. Available at: http://bit.ly/hF9J9r [Accessed 19 July 2010]

Lessig, Lawrence: Free Culture, Penguin, New York, 2004

Levinson, Nanette; Smith, Hank: The Internet Governance Ecosystem: Assessing Multistakeholderism and Change. International Communication Program, School of International Service, American University, Washington 2008

Levy, Steven: Hackers: Heroes of the Computer Revolution, Dell Publishing, New York, 1994

Lewis, James Andrew: Computer Espionage, Titan Rain and China, Center for Strategic and International Studies, Technology and Public Policy Program, Washington DC, December 2005. Available at: http://bit.ly/tPRfyU [Accessed 22 September 2009]

Leyden, John: Bear Prints Found on Georgian CyberAttacks, The Register, 14 August 2008. Available at: http://bit.ly/uc88L6 [Accessed 22 September 2009]

Leyden, John: China Announces Skype Ban to Protect Telco Revenues, The Register, 31 December 2010. Available at: http://bit.ly/gOXNgO [Accessed 14 March 2011]

Li Hongmei: Let go of "WuMaoDang" and "50-cent Party", People's Daily Online, 23 May 2011. Available at: http://bit.ly/sgEu5a [Accessed 11 June 2011]

Linz, Juan J.; Stepan, Alfred: Problems of Democratic Transition and Consolidation. Southern Europe, South America, and Post-Communist Europe. Johns Hopkins University Press, Baltimore 1996

Litman, Jessica: The DNS Wars: Trademarks and the Internet Domain Name System, Journal of Small and Emerging Business Law, 149, 2000, pp. 1-17. Available at: http://bit.ly/dHmyV6 [Accessed 05 June 2009]

Lococo, Edmond; Lee, Mark; MacMillan, Douglas: Facebook Users Dodge Censors to Climb Over China Great Firewall, Bloomberg Businessweek, 17 February 2011. Available at: http://buswk.co/dJwJgC [Accessed 10 December 2008]

Lowe, Graham; Winters, Patrick; Marcus, Michael L.: The Great DNS Wall of China, New York University, 21 December 2007. Available at: http://bit.ly/um4MpQ [Accessed 10 December 2008]

MacKinnon: China's Censorship 2.0: How Companies Censor Bloggers, First Monday, Vol 14, No 2, 2 February 2009. Available at: http://bit.ly/BUbuk [Accessed 05 June 2009]

MacLean, Don: Internet Governance. A Grand Collaboration, UN ICT Task Force, 2004

Malcom, Jeremy: Multi-Stakeholder Governance and the Internet Governance Forum, Terminus Press, Wembley, 2008

Malkin, G.: Internet Users' Glossary, RFC 1983, August 1996. Available at: http://bit.ly/vTHbQq [Accessed 27 May 2009]

Mathiason, John: Internet Governance. The New Frontier of Global Institutions, Routledge, 2009

Markoff, John; Sang-Hun, Choe: Cyberattacks Jam Government And Commercial Websites in U.S. and South Korea, New York Times, 9 July 2009. Available at: http://nyti.ms/rYM0d [Accessed 22 September 2009]

Marsan, Carolyn Duffy: Verisign to bolster .gov security, Network World, 07 February 2011. Available at: http://bit.ly/h5SkSk [Accessed 05 June 2009]

Martens, Jens: Multistakeholder Partnerships – Future Models of Multilateralism? Friedrich Ebert Foundation, Dialogue on Globalization, Occasional Papers, No 29, Berlin, January 2007

Mathiason, John: Internet Governance. The New Frontier of Global Institutions, Routledge, London, 2009

Mathiason, John R.; Kuhlman, Charles C.: International Public Regulation of the Internet: Who Will Give You Your Domain Name?, International Studies Association, Panel on Cyberhype or the Deterritorialization of Politics? The Internet in a Post-Westphalian Order, Minneapolis, 21 March 1998. Available at: http://bit.ly/uEellQ [Accessed 05 June 2009]

Mazarr, Michael: Information Technology and World Politics, Palgrave Macmillan, New York, 2002

McNabb, David E.: Research Methods for Political Science. Quantitative and Qualitative Methods, M.E. Sharpe, London 2004

McQuade III, Samuel C.: Understanding and Managing Cybercrime, Pearson, Boston, 2006

Mehan, Julie E.: Cyberwar, Cyberterror, Cybercrime, IT Governance Publishing Ely, 2008

Messmer, Ellen: Kosovo CyberWar Intensifies: Chinese Hackers Targeting US Sites, Government Says, CNN, 12 May 1999. Available at: http://bit.ly/tnqUNg [Accessed 22 September 2009]

Miegel, Fredrik; Olsson, Tobias: From Pirates to Politicians: The Story of the Swedish File Sharers Who Became a Political Party, in: Carpentier et al: Democracy, Journalism and Technology: New Developments in an Enlarged Europe, Tartu University Press, Tartu, 2008, pp. 203-215. Available at: http://bit.ly/shgPhs [Accessed 25 May 2009]

Miller, Claire Cain: How Obama's Internet Campaign Changed Politics, The New York Times, 7 November 2008. Available at: http://nyti.ms/rwOhn [Accessed 05 June 2009]

Mills, D.L.: Internet Name Domains, RFC 799, September 1981. Available at: http://bit.ly/s5nUpa [Accessed 27 May 2009]

Mockapetris, P.: Domain Names - Concepts and Facilities, RFC 882, November 1983a. Available at: http://bit.ly/tjy0sF [Accessed 17 April 2009]

Mockapetris, P.: Domain Names - Implementation and Specification, RFC 883, November 1983b. Available at: http://bit.ly/tYCyBx [Accessed 17 April 2009]

Modelski, George: Globalization, in: Held, David; McGrew, Anthony: The Global Transformations Reader, Polity Press, Cambridge, 2003, pp. 55-59

Mueller, Milton: ICANN and Internet Governance. Sorting Through the Debris of Self-Regulation, Info, the Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, Vol 1, No 6, December 1999. Available at: http://bit.ly/rIlD6H [Accessed 05 July 2008]

Mueller, Milton: Interview on 14 March 2011. Available at: http://bit.ly/s60sMS

Mueller, Milton: Networks and States. The Global Politics of Internet Governance, MIT Press, Cambridge, 2010

Mueller, Milton: The New Global Politics of Internet Governance, in: Kleinwächter, Wolfgang: The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment, Marketing für Deutschland GmbH, Berlin 2007, pp. 215-219

Mueller, Milton: Ruling The Root, Internet Governance and the Taming of Cyberspace, MIT Press, Cambridge 2002

Mueller, Milton: Taking a Hard Look at the "Affirmation", Internet Governance Project (IGP), 30 September 2009. Available at: http://bit.ly/kg4yB [Accessed 05 June 2009]

Mueller, Milton et al: Political Oversight of ICANN: A Briefing for the WSIS Summit, Concept Paper by the Internet Governance Project, 1 November 2005. Available at: http://bit.ly/ulRsDG [Accessed 22 September 2008]

Mueller, Milton; Mathiason, John; Klein, Hans: The Internet and Global Governance: Principles and Norms for a New Regime, in: Global Governance: A Review of Multilateralism and International Organizations, Vol 13, No 2, April-June 2007, pp. 237-254

Mueller, Milton; Raad, Alexa: Letter to ICANN President Paul Twomey, 29 July 2008. Available at: http://bit.ly/ulRsDG [Accessed 13 April 2009]

Murphy, Craig N.: Global Governance: Poorly Done and Poorly Understood, International Affairs, Vol 76, No 4, October 2000, pp. 789-803

Murphy, Jamie; Elmer-DeWitt, Philip; Krance, Magda: Computers: The 414 Gang Strikes Again, Time Magazine, 29 August 1983. Available at: http://ti.me/7x6FTb [Accessed 29 January 2009]

Murray, Craig: Letter to Professor Bundy, 29 September 2005. Available at: http://bit.ly/ukTDVh [Accessed 09 July 2010]

Musil, Steven: Internet Censorship Plagues Journalists at Olympics. cnet news, 29 July 2008. Available at: http://cnet.co/7vXiWw [Accessed 07 July 2009]

National Science Foundation (NSF): Draft Minutes of the Federal Networking Council Advisory Committee (FNCAC) Meeting, 14-15 April 1997. Available at: http://1.usa.gov/u3PIsC [Accessed 05 June 2009]

National Telecommunications and Information Administration (NTIA): Electronic Filings on Internet Domain Names, Dennis Fazio, Comment No 14, 1 July 1997a. Available at: http://1.usa.gov/w2HDZg [Accessed 05 June 2009]

National Telecommunications and Information Administration (NTIA): Electronic Filings on Internet Domain Names, Edwin Hayward, Comment No 5, 1 July 1997b. Available at: http://1.usa.gov/w2HDZg [Accessed 05 June 2009]

National Telecommunications and Information Administration (NTIA): Electronic Filings on Internet Domain Names, Jesse Kornblum, Comment No 17, 1 July 1997c. Available at: http://1.usa.gov/w2HDZg [Accessed 05 June 2009]

National Telecommunications and Information Administration (NTIA): Improvement of Technical Management of Internet Names and Addresses; Discussion Draft, 30 January 1998a. Available at: http://1.usa.gov/u5bIbe [Accessed 05 June 2009]

National Telecommunications and Information Administration (NTIA): Management of Internet Names and Addresses, Docket Number: 980212036-8146-02, 05 June 1998b. Available at: http://1.usa.gov/tyrxcH [Accessed 05 June 2009]

National Telecommunications and Information Administration (NTIA): Request for Comments on the Registration and Administration of Internet Domain Names, Docket No. 970613137-7137-01, 02 July 1997d. Available at: http://1.usa.gov/tMKyLG [Accessed 05 June 2009]

NDTV: Singham effect: File sharing sites blocked, ndtv.com, 22 July 2011. Available at: http://bit.ly/om4tt4 [Accessed 15 August 2011]

Neef, Christian: Germany's Favorite Despot, Spiegel Online, 8 February 2006. Available at: http://bit.ly/tEoUeV [Accessed 23 August 2009]

Nohlen, Dieter: Lexikon der Politik, Band 2: Politikwissenschaftliche Methoden, C.H. Beck, München, 1994

Nuscheler, Franz: Global Governance, in: Ferdowski, Mir A.: Internationale Politik im 21. Jahrhundert, UTB, München, 2002, pp. 71-85

Nye, Joseph S.: Cyber Insecurity, Project Syndicate, Cambridge, December 2008. Available at: http://bit.ly/vyaYc8 [Accessed 22 September 2009]

Nye, Joseph S.; Kamarck, Elaine Ciulla: Governance.com: Democracy in the Information Age, Brookings Institute Press, Washington D.C, 2002

Organization for Economic Cooperation and Development (OECD): Computer-Related Crime. Analysis of Legal Policy, 31 August 1986

Organization for Economic Cooperation and Development (OECD): Guidelines for the Security of Information Systems and Networks, 2002. Available at: http://bit.ly/nA7yP [Accessed 13 March 2009]

Organization for Economic Cooperation and Development (OECD): Spam Issues in Developing Countries, Task Force on Spam, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 26 May 2005a. Available at: http://bit.ly/v1t3Ne [Accessed 13 March 2009]

Organization for Economic Cooperation and Development (OECD): The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, Working Party on Information Security and Privacy, DSTI/ICCP/REG(2005)1/FINAL, 16 December 2005b. Available at: http://bit.ly/s2gn6K [Accessed 13 March 2009]

Organization for Economic Cooperation and Development (OECD): Understanding the Digital Divide, Paris, 2001. Available at: http://bit.ly/hPLl26 [Accessed 22 June 2009]

OpenNet Initiative (ONI): Internet Filtering in China in 2004-2005: A Country Study. 14 April 2005. Available at: http://bit.ly/vSO5dY [Accessed 22 September 2009]

Oppermann, Daniel: Entre Hackers e Botnets: A Segurança Cibernética no Brasil, Boletim OPSA, No 2, April-June 2011, pp. 12-16. Available at: http://bit.ly/tqsqQD [Accessed 16 October 2011]

Oram, Andy: Peer-to-Peer: Harnessing the Power of Disruptive Technologies, O'Reilly Media, Sebastopol, 2001

Organization of American States (OAS): Final Report of the Fourth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, Port-of-Spain, 10-13 March 2002. Available at: http://bit.ly/sLcamt [Accessed 16 May 2010]

Organization of American States (OAS): Final Report of the Second Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, Lima, 1-3 March 1999. Available at: http://bit.ly/u3WOdK [Accessed 16 May 2010]

Organization of American States (OAS): Final Report of the Third Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, San José, 1-3 March 2000a. Available at: http://bit.ly/sBGthA [Accessed 16 May 2010]

Organization of American States (OAS): Relatório Final da Segunda Reunião de Peritos Governamentais Sobre Delito Cibernético, OEA/Ser.K/XXXIV.3, REMJA-III/doc.9/00, 10 February 2000b. Available at: http://bit.ly/u3WOdK [Accessed 16 May 2010]

Pal, Leslie A.; Teplova, Tatyana: Domain Games: Global Governance of the Internet, in: Oliver, E. Lynn; Sanders, Larry: E-Government Reconsidered: Renewal of Governance for the Knowledge Age, Canadian Plains Research Center, Regina, March 2004

Pattberg, Philipp: The Institutionalisation of Private Governance. Conceptualising an Emerging Trend in Global Environmental Politics, Global Governance Working Paper, Global Governance Project, No 9, Berlin, May 2004

Pierson, David: Father of China's Great Firewall Discusses Being Persona non Grata, Admits to Skirting the Censorship He Built, Los Angeles Times, 17 February 2011. Available at: http://lat.ms/ggNI1Z [Accessed 22 June 2011]

Pigman, Geoffrey Allen: The World Economic Forum. A Multi-Stakeholder Approach to Global Governance, Routledge, Abingdon, 2007

Ponemon Institute: First Annual Cost of Cyber Crime Study, July 2010. Available at: http://bit.ly/bgT0LX [Accessed 10 January 2011]

Postel, J.; Reynolds, J.: Domain Requirements, RFC 920, October 1984. Available at: http://bit.ly/dvjehJ [Accessed 27 May 2009]

Postel, Jon: NCP/TCP Transition Plan, RFC 801, November 1981. Available at: http://bit.ly/sWdNGb [Accessed 27 May 2009]

Postel, Jon: The Domain Names Plan and Schedule, RFC 881, November 1983. Available at: http://bit.ly/rz7kPv [Accessed 27 May 2009]

Postel, Jon; Su, Zaw-Sing: The Domain Naming Convention for Internet User Applications, RFC 819, August 1982. Available at: http://bit.ly/vRRrqB [Accessed 27 May 2009]

Rannut, Mart: Language Policy in Estonia, in: Noves SL, Revista de Sociolingüística, Spring-Summer 2004. Available at: http://bit.ly/AyJTdy [Accessed 05 March 2009]

Raymond, Eric S.: A Brief History of Hackerdom, in: DiBona, Chris; Ockman, Sam; Stone, Mark: Open Sources: Voices from the Open Source Revolution, O'Reilly Media, Sebastopol, 1999, pp. 19-30

Reporters Without Borders (RWB): Burmese Media Combating Censorship, 22 December 2010. Available at: http://bit.ly/hKl4E9 [Accessed 22 August 2011]

Reporters Without Borders (RWB): Internet Enemies, 12 March 2011. Available at: http://bit.ly/dETmno [Accessed 22 June 2011]

Resnick, Paul; Richardson, Caroline; Hanson, Derek: See No Evil: How Internet Filters Affect the Search for Online Health Information, Kaiser Family Foundation, Menlo Park, December 2002. Available at: http://bit.ly/i5EGi8 [Accessed 15 January 2009]

Rhoads, Christopher; Chao, Loretta: Iran's Web Spying Aided By Western Technology, Wall Street Journal, 22 June 2009. Available at: http://on.wsj.com/gzwM4 [Accessed 22 May 2010]

Richards, David L.: Making the National International. Information Technology and Government Respect for Human Rights, in: Allison, Juliann Emmons: Technology, Development, and Democracy. International Conflict and Cooperation in the Information Age, State University of New York Press, Albany, 2002, pp. 161-186

Rieth, Lothar: Der sich wandelnde Mehrwert des UN Global Compact, COP-Projekt I, TU Darmstadt, Juni 2008. Available at: http://bit.ly/tQ5Gcs [Accessed 13 June 2010]

Roberts, J. Timmons; Hite, Amy Bellone: The Globalization and Development Reader, Blackwell Publishing, Oxford, 2007

Roberts, Lawrence G.: Multiple Computer Networks and Intercomputer Communication, June 1967. Available at: http://bit.ly/bgckNl [Accessed 03 September 2008]

Roberts, Paul: Chinese DNS Tampering. A Big Threat To Internet Security, Threatpost, Kaspersky Lab Security News Service, 24 November 2010. Available at: http://bit.ly/gbqz9f [Accessed 14 March 2011]

Rosenau, James N.; Singh, J.P.: Information Technologies and Global Politics, State University of New York Press, Albany, 2002

Rosenau, James N.: Governance in the Twenty-first Century. In: Global Governance 1 (1), 13-43, 1995

Rosenau, James N.; Czempiel, Ernst-Otto: Governance without Government. Order and Change in World Politics. Cambridge University Press, Cambridge 1992

Rosenberg, Richard S.: Controlling Access to the Internet: The Role of Filtering, Ethics and Information Technology, Vol 3, No 1, March 2001, pp. 35–54. Available at: http://bit.ly/s8oD2N [Accessed 15 September 2010]

Rosenzweig, Roy: Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet, The American Historical Review, Vol 103, No 5, December 1998, pp. 1530-1552

Roth, Michele; Senghaas, Dieter: Global Governance für Entwicklung und Frieden: Perspektiven nach einem Jahrzent. Sonderband zum 20-jährigen Bestehen der Stiftung Entwicklung und Frieden. Dietz, Bonn 2006

Rudolf, Peter; Lohmann, Sascha: Amerikanische Iran-Politik unter Barack Obama, SWP-Studie, Stiftung Wissenschaft und Politik, Berlin, August 2010. Available at: http://bit.ly/v1WPCS [Accessed 23 September 2010]

Schmitt, Stefan; Wefing, Heinrich: Stichprobe Deutschland, Zeit Online, 12 November 2010. Available at: http://bit.ly/cZj0Ok [Accessed 19 March 2011]

Schuler, Katharina: Von der Leyen prescht voran, Zeit Online, 26 March 2009. Available at: http://bit.ly/cRHsob [Accessed 14 November 2010]

Schulze, Hendrik; Mochalski, Klaus: Internet Study 2008/2009, Ipoque GmbH, Leipzig, 2009. Available at: http://bit.ly/vvv2dq [Accessed 22 September 2010]

Schwartz, John: Internet Filters Used to Shield Minors Censor Speech, Critics Say, New York Times, 19 March 2001. Available at: http://nyti.ms/vXx8FY [Accessed 14 April 2010]

Skidmore, Monique; Wilson, Trevor: Dictatorship, Disorder and Decline in Myanmar, Australian National University Press, Canberra, 2008. Available at: http://bit.ly/tYq0TE [Accessed 11 April 2010]

Sklair, Leslie: Competing Conceptions of Globalization (1999), in: Roberts, J. Timmons; Hite, Amy Bellone: The Globalization and Development Reader, Blackwell Publishing, Oxford, 2007, pp. 233-246

Smith, Craig S.: May 6-12; The First World Hacker War, New York Times, 13 May 2001. Available at: http://nyti.ms/tPzKVB [Accessed 22 September 2009]

Sommer, Peter; Brown, Ian: Reducing Systemic Cybersecurity Risk, OECD/IFP Project on "Future Global Shocks", 14 January 2011. Available at: http://bit.ly/dNxICx [Accessed 19 May 2011]

Spaink, Karin: Child pornography: Fight It or Hide It? Translation of a column for the Dutch newspaper Het Parool, 19 February 2008. Available at: http://bit.ly/aF0Jh6 [Accessed 14 July 2010]

Spiegel Online: China-Hacker griffen auch britische Regierung an, 5 September 2007a. Available at: http://bit.ly/6oPxM [Accessed 22 September 2009]

Spiegel Online: Chinesische Trojaner auf PCs im Kanzleramt, 25 August 2007b. Available at: http://bit.ly/sKLKY4 [Accessed 22 September 2009]

Spiegel Online: Cyberangriffe auf Estland alarmieren EU und NATO, 17 May 2007c. Available at: http://bit.ly/uHVkBQ [Accessed 22 September 2009]

Spiegel Online: Regierungsbildung in Berlin, Graphics, 2011. Available at: http://bit.ly/r1C0iQ [Accessed 19 November 2011]

Spiegel Online: Schäuble räumt Fehler bei Netzsperren ein, 10 October 2009. Available at: http://bit.ly/iMbCl [Accessed 16 March 2010]

Spiegel Online: Soviet Memorial Causes Rift between Estonia and Russia, 27 April 2007d. Available at: http://bit.ly/nQ7Vo7 [Accessed 22 June 2010]

Stake, Robert E.: Case Studies. In: Denzin, Norman K.; Lincoln, Yvonna S.: Handbook of Qualitative Research, Sage Publications, London, 1994

Stevens, Tim: The Internet Smokescreen, Open Democracy, 21 August 2008. Available at: http://bit.ly/sprZKa [Accessed 22 September 2009]

Stiftung Wissenschaft und Frieden: Global Governance für Entwicklung und Frieden, Dietz, Bonn, 2006

Stine, Deborah D.: U.S. Civilian Space Policy Priorities: Reflections 50 Years After Sputnik, CRS Report for Congress, 2 February 2009. Available at: http://bit.ly/rO0rZe [Accessed 05 June 2009]

Stol et al: Governmental Filtering of Websites: The Dutch Case, in: Computer Law & Security Review, Vol 25, No 3, 2009, pp. 251-262. Available at: http://bit.ly/a9hTPC [Accessed 05 June 2009]

Streitfeld, David: In a Race to Out-Rave, 5-Star Web Reviews Go for $5, New York Times, 19 August 2011. Available at: http://nyti.ms/rdwKh5 [Accessed 15 September 2011]

Sueddeutsche.de: Chinesische Hacker greifen Pentagon an, 4 September 2007b. Available at: http://bit.ly/suPaJH [Accessed 22 September 2009]

Sueddeutsche.de: Jugendliche greifen estnische Botschafterin an, 2 May 2007a. Available at: http://bit.ly/uILIXc [Accessed 22 September 2009]

Sueddeutsche.de: Web-Sperren gegen Kinderpornografie gebilligt. 18 June 2009. Available at: http://bit.ly/sZC56 [Accessed 18 July 2009]

Sueddeutsche.de: Wowereit kann in Berlin weiterregieren - FDP stürzt ab, 18 September 2011. Available at: http://bit.ly/oW8RNv [Accessed 12 October 2011]

Svantesson, Dan Jerker B.: Privacy, the Internet and Transborder Data Flows. An Australian Perspective, Masaryk University Journal of Law and Technology, Vol 4, No 1, 2010. Available at: http://bit.ly/u3LtrE [Accessed 13 December 2010]

Tagesspiegel: Stopp-Schilder für Kinderpornos im Internet, 17 April 2009. Available at: http://bit.ly/trgG1c [Accessed 27 December 2009]

The Economist: ICANN be independent. America is poised to loosen its control over cyberspace, 24 September 2009. Available at: http://econ.st/tbBS1q [Accessed 05 June 2009]

The White House: The Framework for Global Electronic Commerce, 1997. Available at: http://1.usa.gov/rZUWiy [Accessed 14 March 2008]

Thomas, Timothy L.: Like Adding Wings to the Tiger: Chinese Information War Theory and Practice, Foreign Military Studies Office Publications, 2000. Available at: http://bit.ly/va7Yed [Accessed 20 September 2009]

Thornburgh, Nathan: Inside The Chinese Hack Attack, Time.com, 25 August 2005. Available at: http://ti.me/85LGbb [Accessed 20 September 2009]

United Nations (UN): Combating the Criminal Misuse of Information Technologies, Resolution A/RES/55/63, 22 January 2001. Available at: http://bit.ly/F514Q [Accessed 13 May 2011]

United Nations (UN): Combating the Criminal Misuse of Information Technologies, Resolution A/RES/56/121, 23 January 2002a. Available at: http://bit.ly/F514Q [Accessed 13 May 2011]

United Nations (UN): Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime, Report of the Secretary-General, Economic and Social Council, E/CN.15/2001/4, 30 March 2001. Available at: http://bit.ly/F514Q [Accessed 13 May 2011]

United Nations (UN): Draft Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, 12th United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.213/L.6/Rev.2, Salvador, Brazil, 12-19 April 2010. Available at: http://bit.ly/F514Q [Accessed 13 May 2011]

United Nations (UN): Effective Measures to Prevent and Control Computer-Related Crime, Report of the Secretary-General, Economic and Social Council, E/CN.15/2002/8, 29 January 2002b. Available at: http://bit.ly/F514Q [Accessed 13 May 2011]

United Nations (UN): Manual on the Prevention and Control of Computer-Related Crime, International Review of Criminal Policy, No 43/44, 1994. Available at: http://bit.ly/ttKH1w [Accessed 13 May 2011]

United Nations (UN): Report of the Asia and Pacific Regional Preparatory Meeting For the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, A/Conf.144/RPM.1, 16 May 1989. Available at: http://bit.ly/tbWXNm [Accessed 13 July 2010]

United Nations (UN): Security Council Resolution 1308, S/RES/1308 (2000), 17 July 2000. Available at: http://bit.ly/x5Q9oG [Accessed 13 May 2011]

United States District Court: Mainstream Loudoun v. Board of Trustees of the Loudon County Library (E.D. Va. 1998), 24 F. Supp. 2d 552, 23 November 1998. Available at: http://bit.ly/tbWXNm [Accessed 27 April 2011]

United States District Court: Melvin I. Urofsky v. George Allen, Governor of the Commonwealth of Virginia, Civil Action No. 97-701-A, 26 February 1998. Available at: http://bit.ly/tSldO3 [Accessed 27 April 2011]

United States District Court: Plaintiff v. The People's Republic of China, Case No. CV10-0038, Central District of California - Western Division, 5 January 2010. Available at: http://bit.ly/7q54kA [Accessed 27 April 2011]

UNODC: The Globalization of Crime. A Transnational Organized Crime Threat Assessment, United Nations Office on Drugs and Crime, 2010. Available at: http://bit.ly/99HPqw [Accessed 13 May 2011]

U.S.-China Economic and Security Review Commission (USCC): Report to Congress 2010, November 2010. Available at: http://bit.ly/ad3ucL [Accessed 15 April 2011]

U.S. House of Representatives: Internet Domain Names Part 1, Committee on Science, Subcommittee on Basic Research, Washington D.C., 25 September 1997. Available at: http://1.usa.gov/tkbNf3 [Accessed 05 June 2009]

Väyrynen, Raimo: Globalization and Global Governance, Rowman and Littlefield Publishers, Lanham, 1999

VeriSign: Investor Relations, Fact Sheet, s.d. Available at: http://bit.ly/uooWwx [Accessed 05 June 2009]

Vetik, Raivo: Ethnic Conflict and Accommodation in Post-Communist Estonia, in: Journal of Peace Research, Vol 30, No 3, 1993, pp. 271-280

Wacker, Gudrun: Hinter der virtuellen Mauer: Die VR China und das Internet, Bundesinstitut für Ostwissenschaftliche und Internationale Studien, Köln 2000. Available at: http://bit.ly/t053iP [Accessed 20 September 2009]

Wagner, Ben: Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control', Global Voices, 2009. Available at: http://bit.ly/2eMt2F [Accessed 25 April 2010]

Wahlumfrage: 6 aktuelle Wahlumfragen im Vergleich – Bundestag (20.10.11), October 2011. Available at: http://bit.ly/reRwum [Accessed 12 November 2011]

Waldman, Amy: Nepal's King Cracks Down on Politics and News Media, New York Times, 8 February 2005. Available at: http://nyti.ms/vWfovS [Accessed 15 November 2009]

Wall, David S.: Cybercrime, Polity Press, Cambridge, 2007

Walton, Greg: China's Golden Shield, International Centre for Human Rights and Democratic Development, 2001. Available at: http://bit.ly/N4O9p [Accessed 22 October 2009]

Ward, Mark: Big Push for Chinese Net Domains, BBC, 3 March 2006. Available at: http://bbc.in/smBlHl [Accessed 12 May 2009]

Warren, Peter: Hunt For Russia's Web Criminals, Guardian, 15 November 2007. Available at: http://bit.ly/vjWQvM [Accessed 20 September 2009]

Waterman, Shaun: Georgia Blames Russia for Cyberattack on Web Sites, Cell Phones, UPI.com, 11 August 2008. Available at: http://bit.ly/4tP9UR [Accessed 20 September 2009]

Watts, Jonathan: Microsoft Helps China to Censor Bloggers, The Guardian, 15 June 2005. Available at: http://bit.ly/s1RYU4 [Accessed 13 July 2009]

Watts, Jonathan; Branigan, Tania: China Delays Launch of Internet Filter Green Dam, The Guardian, 30 June 2009. Available at: http://bit.ly/163b2n [Accessed 13 July 2009]

Weimann, Gabriel: Terror on the Internet, United States Institute of Peace, Washington D.C., 2006

Welch, Dylan: Coalition Rejects Internet Filter, The Sydney Morning Herald, 6 August 2010. Available at: http://bit.ly/tk5vBt [Accessed 11 December 2010]

Willsher, Kim: Sarkozy opens 'historic' forum on future of internet in runup to G8, The Guardian, 24 May 2011. Available at: http://bit.ly/uy0IU1 [Accessed 05 June 2009]

Wines, Michael: After Outcry, China Delays Requirement for Web-Filtering Software, New York Times, 30 June 2009. Available at: http://nyti.ms/jBqr5 [Accessed 24 May 2010]

WGIG: Background Report, June 2005a. Available at: http://bit.ly/sojgVw [Accessed 22 May 2009]

WGIG: Report of the Working Group on Internet Governance, Château de Bossey, June 2005b. Available at: http://bit.ly/dxGmEp [Accessed 18 July 2009]

Wolchok, Scott; Yao, Randy; Halderman, J. Alex: Analysis of the Green Dam Censorware System, Computer Science and Engineering Division, University of Michigan, 11 June 2009. Available at: http://bit.ly/sWkw75 [Accessed 15 July 2009]

Wolfgarten, Sebastian: Investigating Large-Scale Internet Content Filtering, Dublin City University, 2006. Available at: http://bit.ly/u72G2f [Accessed 22 May 2009]

Woods, Ngaire: Global Governance and the Role of Institutions. In: Held, David; McGrew, Anthony: Governing Globalization. Polity Press, Cambridge 2002

Woyke, Wichard: Handwörterbuch Internationale Politik, Leske und Budrich, Opladen, 1995

WSIS: Geneva Declaration of Principles, WSIS-03/GENEVA/DOC/0004, 12 December 2003a. Available at: http://bit.ly/vNs6xW [Accessed 18 July 2009]

WSIS: Geneva Plan of Action, WSIS-03/GENEVA/DOC/5-E, 12 December 2003b. Available at: http://bit.ly/vNs6xW [Accessed 18 July 2009]

WSIS: Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev.1)-E, 18 November 2005. Available at: http://bit.ly/tAnjdR [Accessed 13 July 2009]

Yin, Robert K.: Case Study Research: Design and Methods, Sage Publications, London, 2003

Young, Oran R.: Global Governance. Drawing Insights from the Environmental Experience, MIT Press, Cambridge, 2000

Zetter, Kim: How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, Wired, 11 July 2011. Available at: http://bit.ly/qI9TFI [Accessed 13 August 2011]

Zhang Lei: Invisible Footprints of Online Commentators, Global Times, 05 February 2010. Available at: http://bit.ly/tNTWgc [Accessed 25 March 2010]